AntiVirus with Spy Sweeper 2011

User Guide

Webroot Software, Inc.
PO Box 19816
Boulder, CO 80308

www.webroot.com

Version 7.0.9

Webroot AntiVirus with Spy Sweeper User Guide

Version 7.0.9; March 31, 2011

Contents

1: Getting Started

This guide describes how to use the Webroot® AntiVirus with Spy Sweeper® (WAVSS) software. This Webroot software combines the #1 antispyware technology with industry-leading antivirus protection for complete security.

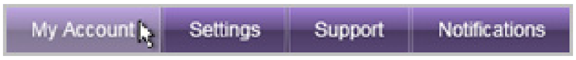
To get started using the Webroot software, see the following topics:

Creating a Webroot account

Your Webroot account includes your software license status and provides access to certain tasks, such as upgrading your software and installing it on another computer (if you purchased a multi-user license). The account is available online through *My Webroot*, which is your personalized Web site available 24 hours a day, every day of the year.

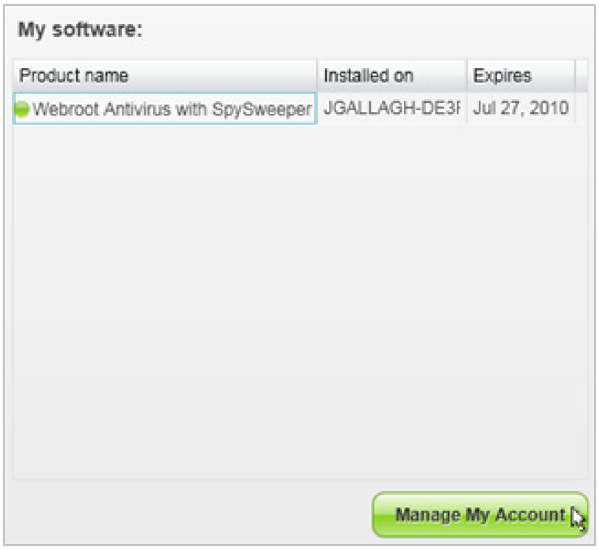
To create a Webroot account:

1. Make sure you are connected to the Internet.
2. Open the Webroot main interface by double-clicking the Webroot icon in the system tray.
3. From the taskbar at bottom of the Home panel, click **My Account**.



The My Account panel opens and shows your keycode, version number, and other information about your subscription.

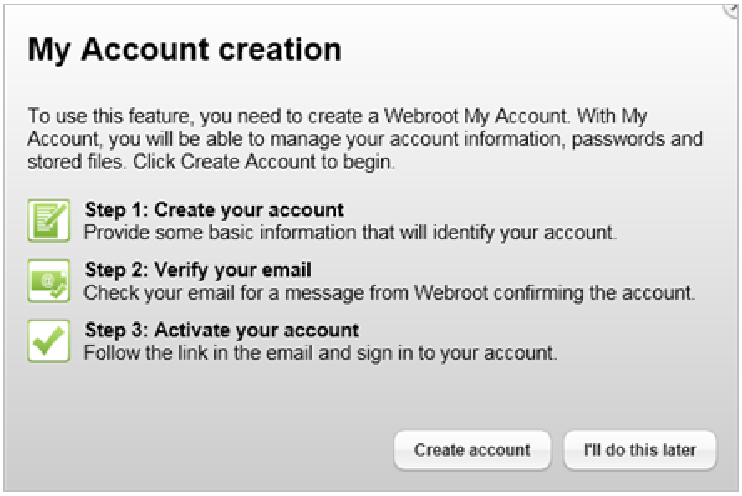
4. Click the **Manage My Account** button at the bottom of the panel.



My software:

Product name	Installed on	Expires
● Webroot Antivirus with SpySweeper	JGALLAGH-DE3I	Jul 27, 2010

If you have not previously created an account, an account creation dialog opens, as shown in the following example. (If you have previously created an account, the *My Webroot* site opens in a browser and you do not need to follow these instructions.)



My Account creation

To use this feature, you need to create a Webroot My Account. With My Account, you will be able to manage your account information, passwords and stored files. Click Create Account to begin.

Step 1: Create your account
Provide some basic information that will identify your account.

Step 2: Verify your email
Check your email for a message from Webroot confirming the account.

Step 3: Activate your account
Follow the link in the email and sign in to your account.

5. Click the **Create account** button and follow the on-screen instructions.

Note

The Webroot software blocks certain terms in user names, such as obscene words. If you use a term on our "blocked" list, your account creation may be rejected. If you experience problems creating an account, contact Webroot Support.

When you complete the account creation process, your account information is provided online through *My Webroot*, which is your personalized Web site available 24 hours a day, every day of the year.

6. To access *My Webroot*, you can click the **Manage My Account** button again. You can also open a Web browser and enter https://www.webroot.com/mywebroot in the address bar. When the Sign In dialog opens, enter your user name and password.

Note

If you did not complete all the steps above or if you did not enter a valid email address, account creation will fail. If this happens, you can complete the process by following steps 1-4 above. When a dialog opens that says your account has not been activated, click the **Activate account** button and follow the on-screen instructions that open in your Web browser.

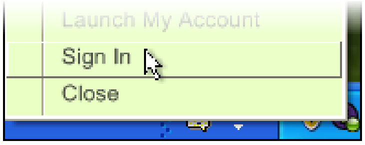
Signing in to your Webroot account

You can log in to your Webroot account to access software license information and perform certain tasks, such as upgrading your software and installing it on another computer (if you purchased a multi-user license). The account is available online 24 hours a day, every day of the year from *My Webroot* (see “Using My Webroot” on page 11).

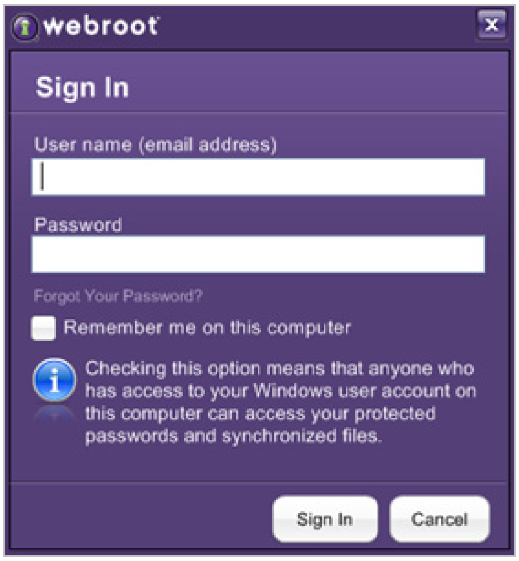
If you have not yet created an account, see “Creating a Webroot account” on page 2.

To sign in to your Webroot account:

1. Right-click the Webroot icon in the system tray and click **Sign In** from the pop-up menu.



The Sign In dialog opens.



Checking this option means that anyone who has access to your Windows user account on this computer can access your protected passwords and synchronized files.

2. Enter your user name (your email address) and password, then click the **Sign In** button.

   You can now access your online account (see “Using My Webroot” on page 11).

Note

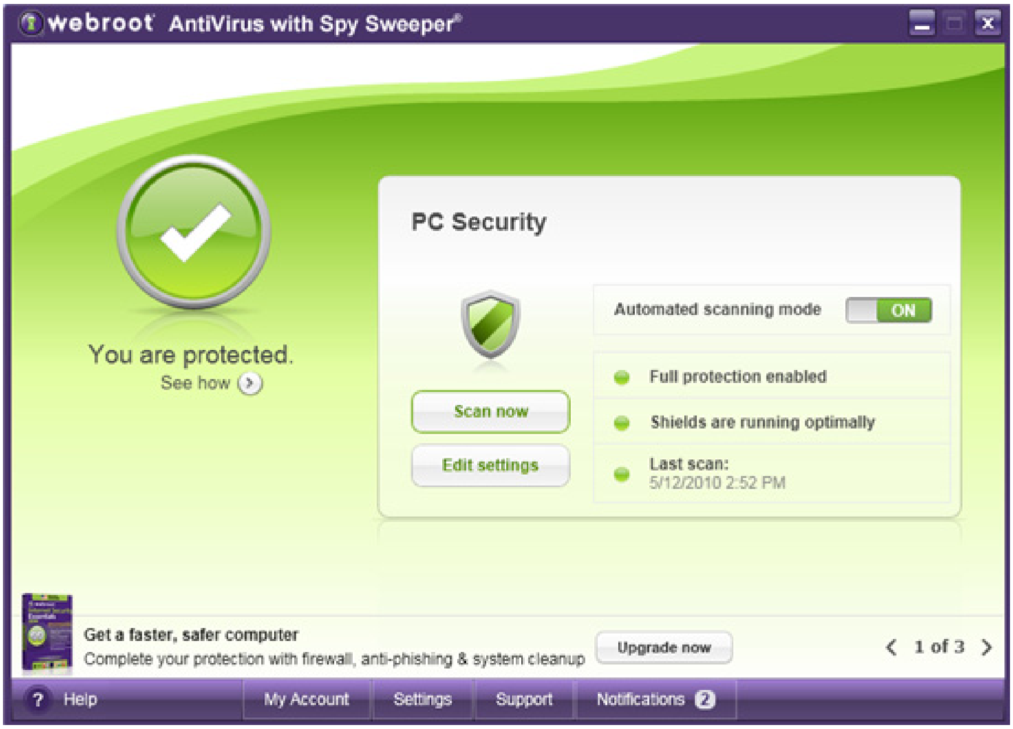
If you cannot remember your account password, click **Forgot Your Password?**. In the dialog that opens, enter your email address and click **Send Email**. Webroot sends a message to your email address with instructions for resetting your password.

Using the main interface

If you want to check on system status or change some settings, you can open the Webroot software's main interface by doing either of the following:

- Double-click the Webroot icon in the system tray. The system tray is located in the lower right corner of your computer screen desktop.
- Open the Windows **Start** menu, click **All Programs** (or **Programs**), click **Webroot**, then click the name of your Webroot software version.
- Double-click the Webroot icon on your Windows desktop:

The main interface opens and displays the Home panel, which provides access to all functions and notifications for the Webroot software.



Automated scanning mode ON

Full protection enabled

Shields are running optimally

Last scan: 5/12/2010 2:52 PM

Get a faster, safer computer
Complete your protection with firewall, anti-phishing & system cleanup

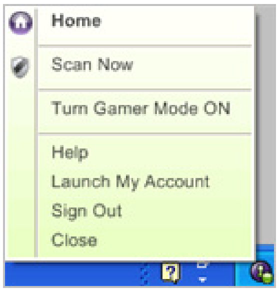
Home panel	
Status color (green, yellow, or red)	Green: Your computer is secure. Yellow: A message requires your attention. Red: A critical item requires your intervention.
See how button	Opens another panel that shows a status of your computer's security.
Scan now button	Launches the System Scanner. See "Scanning for threats" on page 14.
Edit settings button	Opens another panel where you can change settings for scans. See "Customizing scan options" on page 19.

Home panel ***(continued)***	
Help	Opens the main Help file.
My Account	Opens the My Account panel, where you can view subscription information and access a link for managing your account in *My Webroot*. See Chapter 5, “My Account Management” on page 39.
Settings	Opens the Settings panel, where you can modify scanning schedules, view the system history, set program update options, set Gamer mode, and specify settings for a proxy server. See Chapter 6, “Program Settings” on page 45.
Support	Opens the Support panel, which provides Webroot Technical numbers and links.
Notifications	Opens the Notifications panel, which provides a list of status alerts. See “Responding to notifications” on page 10.

Using the Webroot system tray menu

After you install the Webroot software, a Webroot icon opens in the Windows system tray, located in the bottom right of your computer desktop. This icon provides access to Webroot’s system tray menu and some common Webroot functions.

To open the system tray menu, right-click on the Webroot icon .



The menu provides the following selections:

System Tray Menu	
Home	Launches the main interface.
Scan Now	Launches the System Scanner. The icon changes to a Busy state . See “Scanning for threats” on page 14.
Turn ON/OFF Gamer Mode	Turns Gamer mode on or off. See “Setting Gamer mode” on page 50.
Help	Launches the main Help file.
Launch My Account	Launches an Internet browser and opens *My Webroot*. See “Using My Webroot” on page 11.

System Tray Menu *(continued)*	
Sign In/Sign Out	If you are not signed in to your Webroot account, this selection displays “Sign In” and launches a dialog window for you to enter your name and password to access your account. If you are signed in already, this selection displays “Sign Out” and logs out of your account.
Close	Closes the Webroot software main interface. **Note**: Selecting “Close” does not stop currently active or scheduled tasks, such as scans.

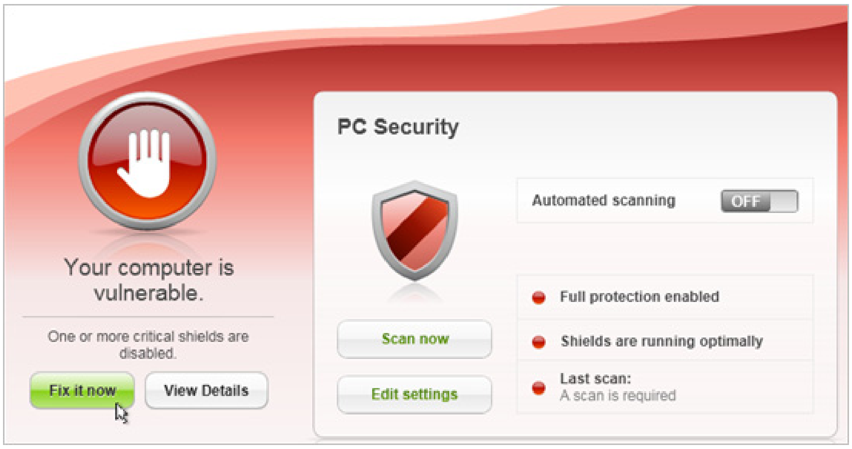
Viewing protection status

To show your computer’s overall protection status, areas of the Webroot user interface change colors, as follows:

Main Interface Color	Icon	Description
Green	🟢	Your computer is secure.
Yellow	🟡	One or more messages require your attention.
Red	🔴	One or more critical items require your intervention.

To view protection status:

1. Open the Home panel of the Webroot software’s main interface by double-clicking the Webroot icon in the system tray.
2. From the Home panel, you can read a short description about the issue.



Your computer is vulnerable.

One or more critical shields are disabled.

PC Security

Automated scanning OFF

● Full protection enabled

● Shields are running optimally

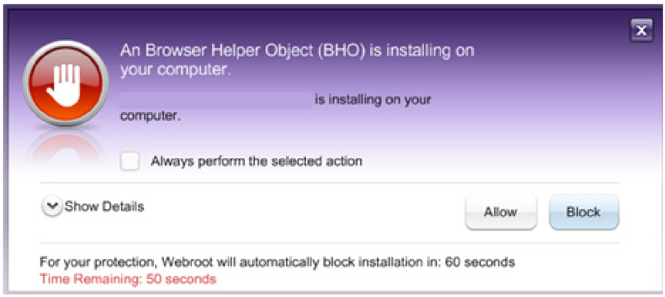
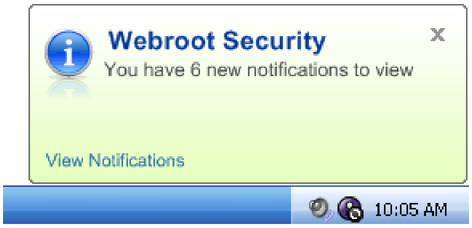
● Last scan: A scan is required

The panel may also provide buttons for how to fix the issue or how to view more detailed information:

- **Fix it now**. The Webroot software will resolve the situation. The action it takes depends on the issue. For example, if you turned off an important shield, it will turn it back on.
- **View Details**. The Webroot software opens a panel where you can view more information and fix the issue.

Responding to alerts

If the Webroot software needs to inform you about an important system status, it opens a pop-up alert in the middle of your computer screen or a balloon alert from the system tray, as follows:

Alert methods	
Pop-up alerts Appear in the middle of the computer screen and require immediate action. See “Responding to pop-up alerts” after this table.	 An Browser Helper Object (BHO) is installing on your computer. is installing on your computer. □ Always perform the selected action For your protection, Webroot will automatically block installation in: 60 seconds Time Remaining: 50 seconds
Balloon alerts Open from the system tray and may be informational or require action. See “Responding to balloon alerts” on page 9.	 Webroot Security You have 6 new notifications to view

Responding to pop-up alerts

The Webroot software opens a pop-up alert when it detects an item trying to download to your computer and it cannot determine whether this item is a threat or a legitimate program. For example, the Webroot Shields may open an alert if you are downloading a new toolbar for your browser. Toolbars are classified as Browser Helper Objects (BHOs), and although most BHOs are legitimate, some are part of spyware that can download without your knowledge. Because Webroot cannot determine if you want this toolbar, you need to respond by selecting **Allow** or **Block**. If you do not respond within the allotted time shown in the alert counter (usually 60 seconds), the Webroot Shields automatically block the activity.

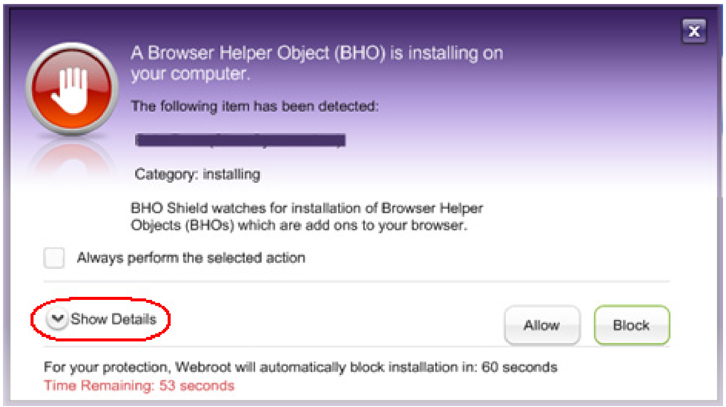
Note

If a pop-up alert opens and you aren’t certain whether to allow or block the detected item, your safest action is to block it. The name of the file trying to download is displayed in the alert box. Click **Show Details** for more information or contact Webroot Support.

To respond to pop-up alerts:

1. Read the alert text to determine what type of program is attempting to download to your computer. You can click the arrow next to **Show Details** to view the name, file name, company, and copyright of the program.

   The following example shows an alert detected by the Webroot Shields.



A Browser Helper Object (BHO) is installing on your computer.

The following item has been detected:

[redacted]

Category: installing

BHO Shield watches for installation of Browser Helper Objects (BHOs) which are add ons to your browser.

☐ Always perform the selected action

For your protection, Webroot will automatically block installation in: 60 seconds
Time Remaining: 53 seconds

2. Click the **Block** button if you do not recognize the program and were not trying to download anything as you viewed pages on the Internet.
   or
   Click the **Allow** button if you do recognize the program and you are purposely downloading it.

Note

Some alerts provide an **Always perform the selected action** checkbox. If Webroot frequently detects the same item, you can select this checkbox so Webroot will always allow or block the item in the future.

Responding to balloon alerts

If the Webroot software needs to report important system status or an issue that requires your attention, it opens a balloon alert near the Webroot icon in the system tray. These alerts are only visible for a short time (maximum 30 seconds) depending on the level of importance:

- **Information only**: Appears for 10 seconds and provides status information. You do not need to take action.
- **Action**: Appears for 15 seconds and provides a link for you to click and view more information. These alerts require you to take action to resolve an issue.
- **Critical action**: Appears for 20 to 30 seconds and provides a link for you to click and view more information. These alerts require you to take action to resolve a critical issue.

To respond to balloon alerts:

1. If you notice a link in the balloon alert, such as **View Notifications**, click the link.

   The Webroot software's main interface opens with the Notifications panel displayed.

2. Take action for each alert displayed in the Notifications panel. For further instructions, see "Responding to notifications" on page 10.

Note

If the alert disappears before you can click on the link, open the main interface (double-click the Webroot icon in the system tray), then click **Notifications** at the bottom taskbar. The Notifications panel shows all alerts that require your attention.

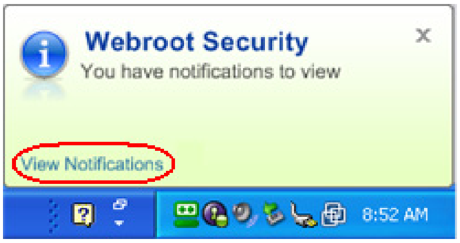
Responding to notifications

The Notifications panel shows alerts that may require you to take an action. Depending on the issue, the notification includes instructions and buttons that guide you to managing and resolving the issue.

To respond to notifications:

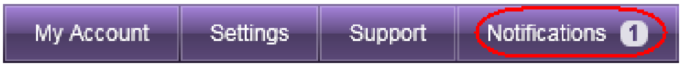
1. Open the Notifications panel by doing either of the following:

   - From the system tray, click the **View Notifications** link from an alert balloon.



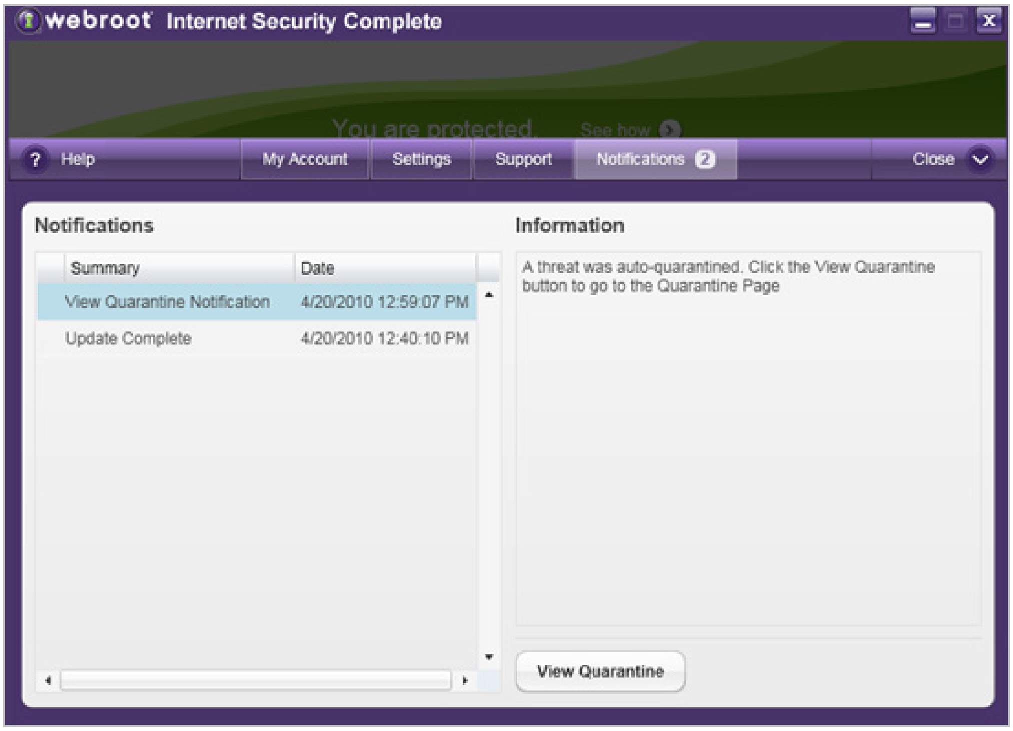
   -or -

   - From the main interface's Home panel, click **Notifications** in the bottom taskbar.



   The Notifications panel opens.

2. Click on an item in the Summary pane to display more information at the right.



Summary	Date
View Quarantine Notification	4/20/2010 12:59:07 PM
Update Complete	4/20/2010 12:40:10 PM

A threat was auto-quarantined. Click the View Quarantine button to go to the Quarantine Page

3. Read the details description and respond by clicking links or buttons for your desired action.

For some types of notifications, you can select the checkbox for **Always perform the selected action**, so you do not need to respond to the same alert again.

Once you respond to a notification, it no longer appears in the Notifications panel and is moved to the History panel (under Settings). See "Viewing the system history" on page 47.

Using *My Webroot*

My Webroot is your personalized Webroot Web site that is available 24 hours a day, every day of the year. From *My Webroot*, you can log in to your Webroot account to access your software license status and certain tasks, such as upgrading your software and installing it on another computer (if you purchased a multi-user license). You can access *My Webroot* from any computer.

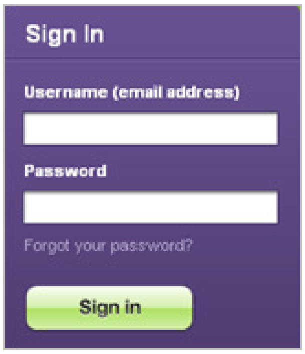
Note

You must create an account to access *My Webroot*. If you have not yet created an account, see "Creating a Webroot account" on page 2.

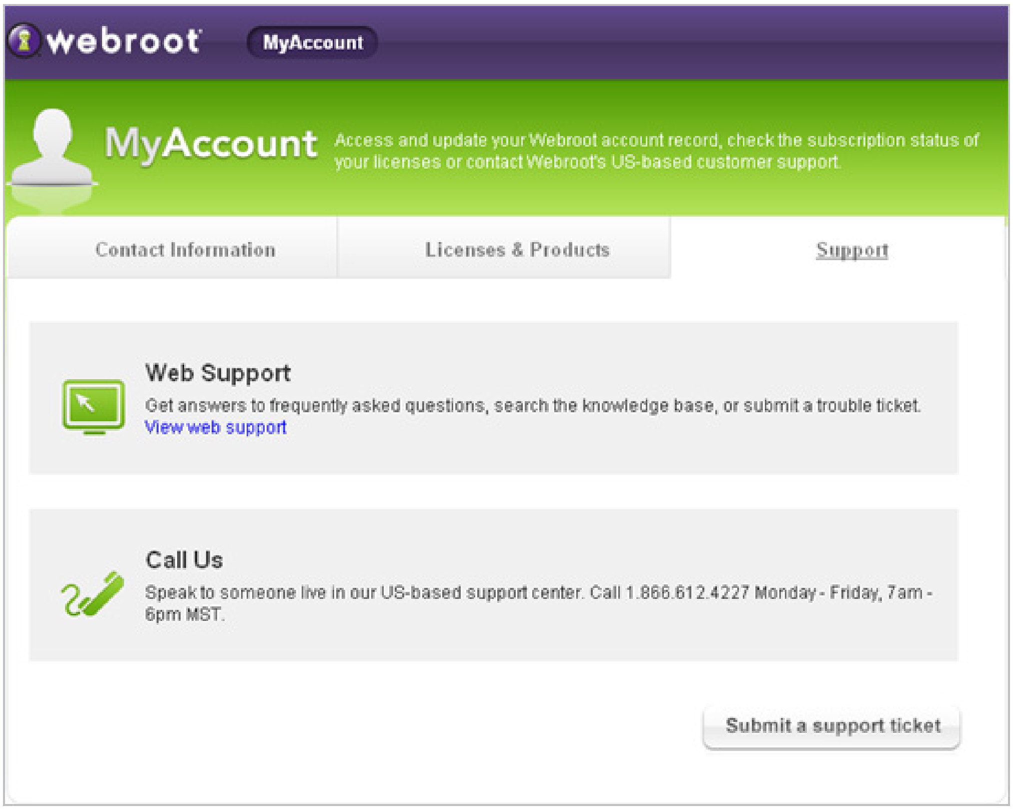
You can open *My Webroot* by doing either of the following:

- Open your browser and enter https://www.webroot.com/mywebroot.
- Open the main interface (double-click the Webroot icon in the system tray). From the taskbar at bottom of the Home panel, click **My Account**. When the My Account panel opens, click the **Manage My Account** button.

If you are not signed in already, *My Webroot* opens with a Sign In panel on the right, as shown below. Enter your user name (email address) and password, then click the **Sign in** button.



If you are signed in, Webroot bypasses this screen and goes directly to your account.



MyAccount

Access and update your Webroot account record, check the subscription status of your licenses or contact Webroot's US-based customer support.

Web Support

Get answers to frequently asked questions, search the knowledge base, or submit a trouble ticket.

Call Us

Speak to someone live in our US-based support center. Call 1.866.612.4227 Monday - Friday, 7am - 6pm MST.

The following table describes the pages available in *My Webroot*.

***My Webroot* pages**	
Home	Serves as the main dashboard to all *My Webroot* functions available with your subscription and license.
MyAccount	Shows your account details and software license information. See Chapter 5, "My Account Management" on page 39.

Note

If you install a new browser later (*after* installing the Webroot program), the Webroot toolbar will not appear in that browser until the next program update. If you want to install the Webroot toolbar right away, close your browser, then go to the Windows **Start** menu, select **All Programs** (or **Programs**), **Webroot**, **Tools**, **Install Webroot Toolbar**. Webroot will download and install the toolbar.

2: Security Scans

The System Scanner searches all areas of your computer where potential threats can hide, including drives, files, the Windows registry, and system memory. It looks for any files or other items that match our security definitions (a set of fingerprints that characterize potential threats). When it detects items, it takes one of the following actions:

- For definite threats (positive matches with security definitions), the System Scanner removes the items from their current locations and sends them to a holding area, called Quarantine, where they are rendered inoperable and cannot cause any harm.
- For programs that are classified as "potentially unwanted applications," the System Scanner opens a notification about what it found. You can decide whether to send the item to Quarantine or ignore it.
- For viruses, the System Scanner removes the infected portions of the file during a cleaning process. It keeps the cleaned file in its original location and sends a copy of the corrupted file to Quarantine.

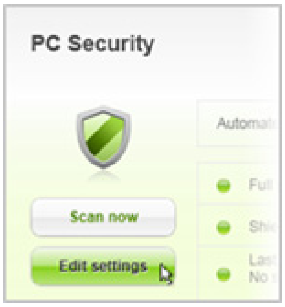
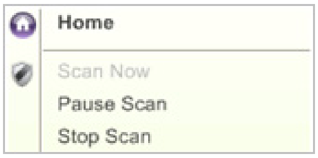
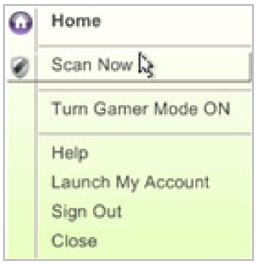
The System Scanner is preconfigured to scan your computer automatically at optimal times, without disrupting your work. You can also disable automated scanning and run the System Scanner manually.

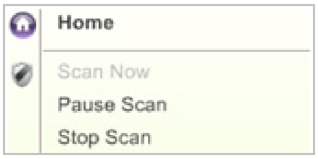
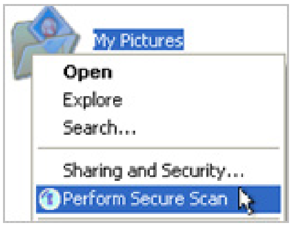
To use the System Scanner, see the following topics:

- "Scanning for threats" on page 14
- "Viewing scan details" on page 16
- "Customizing scan options" on page 19
- "Creating a scan schedule" on page 21

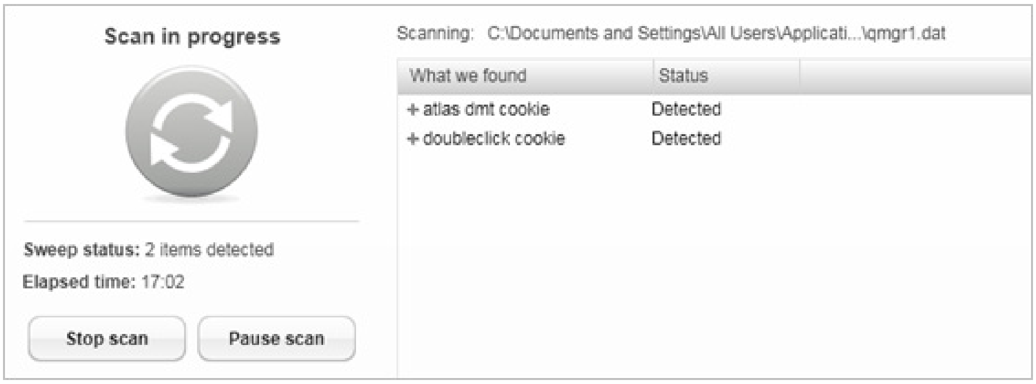
Scanning for threats

Although the System Scanner is preconfigured for automated scanning, you can run an immediate scan yourself at any time. You can start a scan from the Webroot software's main interface, from the system tray menu, or from Windows Explorer.

Methods for launching a manual scan		
Main interface	**To run a scan from the main interface**: 1. Open the Webroot main interface by double-clicking the Webroot icon in the system tray. 2. Click the **Scan now** button in the PC Security panel. **To view its progress or to stop the scan:** The Scan in Progress panel opens. You can stop or pause the scan by selecting either the **Stop Scan** or **Pause Scan** buttons.	 PC Security Automat Scan now Edit settings Ful Shi Las No
System tray menu	**To run a scan from the system tray:** 1. Open the Webroot main interface by double-clicking the Webroot icon in the system tray. 2. Click **Scan Now**. The Webroot icon displays a turning dial to indicate it's busy scanning: . During the scan, the system tray menu provides additional options for pausing or stopping the scan.  If you want to see scan details, click **Home**. The Scan in Progress panel opens (see the illustration below this table).	 Home Scan Now Turn Gamer Mode ON Help Launch My Account Sign Out Close

Methods for launching a manual scan *(continued)*		
Windows Explorer	**To run a scan from Windows Explorer:** 1. Open Windows Explorer. 2. Right-click the file, folder, or drive you want to scan. From the pop-up menu, select **Perform Secure Scan**. The system tray icon displays a turning dial to indicate it's busy scanning: . During the scan, the system tray menu provides additional options for pausing or stopping the scan.  If you want to see scan details, click Home. The Scan in Progress panel opens (see the illustration below this table).	 My Pictures Open Explore Search... Sharing and Security... Perform Secure Scan

The Scan in Progress panel shows the items as they are detected.



Sweep status: 2 items detected

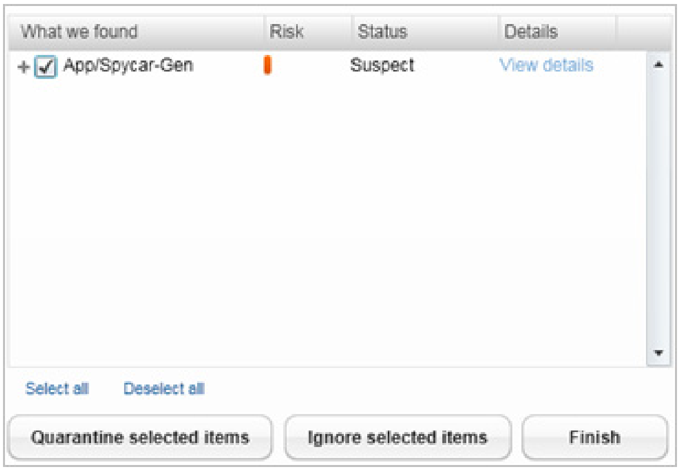
Elapsed time: 17:02

Scanning: C:\Documents and Settings\All Users\Applicati...\qmgr1.dat

What we found	Status
+ atlas dmt cookie	Detected
+ doubleclick cookie	Detected

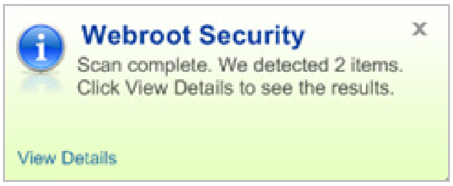
When the scan completes, the Webroot software takes one of the following actions:

- For definite threats (positive matches with security definitions), the System Scanner removes the items from their current locations and sends them to a holding area, called Quarantine, where they are rendered inoperable and cannot cause any harm. The Status changes to “Quarantined.” For more information, see Chapter 3, “Quarantine” on page 23.
- For viruses, the System Scanner removes the infected portions of the file during a cleaning process. It keeps the cleaned file in its original location and sends a copy of the corrupted file to Quarantine. The status changes to “Cleaned.”
- For programs that are classified as “potentially unwanted applications,” the System Scanner does not automatically quarantine the items. Instead, it marks the status as “Suspect,” as shown in the following example. You must take action yourself by selecting the item in the panel and choosing either the **Quarantine selected items** or **Ignore selected items** button.



What we found	Risk	Status	Details
+ ☑ App/Spycar-Gen	▮	Suspect	View details

After the Webroot software manages the items, it opens a notification in the system tray. You can click **View Details** to see more information about what items were quarantined. (If the alert closes before you have a chance to click the link, point your mouse to the PC Security panel, click the **Edit settings** button, then click **View scan details** in the Scan tab.)



Webroot Security

Scan complete. We detected 2 items. Click View Details to see the results.

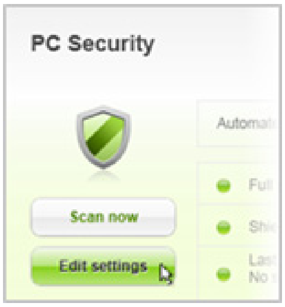
See the next section, "Viewing scan details," for more information.

Viewing scan details

You can view results of the last scan from the Scan panel.

To view scan details:

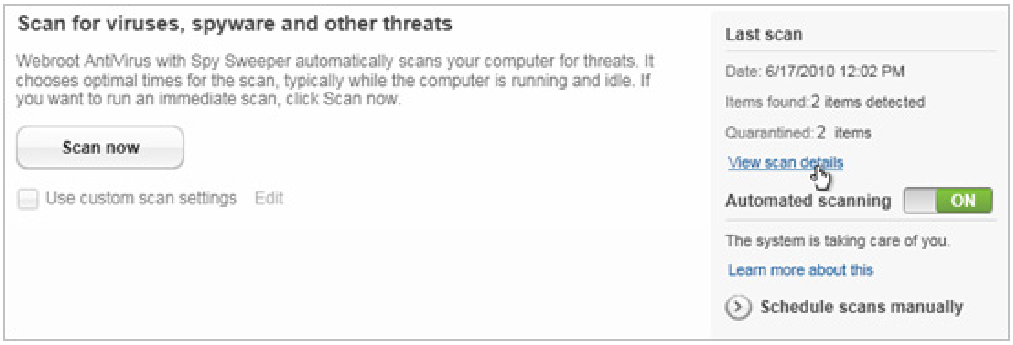
1. Open the Webroot main interface by double-clicking the Webroot icon in the system tray.
2. From the Home panel, click the **Edit settings** button under PC Security.



The PC Security panel opens.

3. Make sure the **Scan** tab is selected.

4. Under **Last scan**, click **View scan details**.



Scan for viruses, spyware and other threats

Webroot AntiVirus with Spy Sweeper automatically scans your computer for threats. It chooses optimal times for the scan, typically while the computer is running and idle. If you want to run an immediate scan, click Scan now.

Scan now

□ Use custom scan settings Edit

Last scan

Date: 6/17/2010 12:02 PM

Items found: 2 items detected

Quarantined: 2 items

View scan details

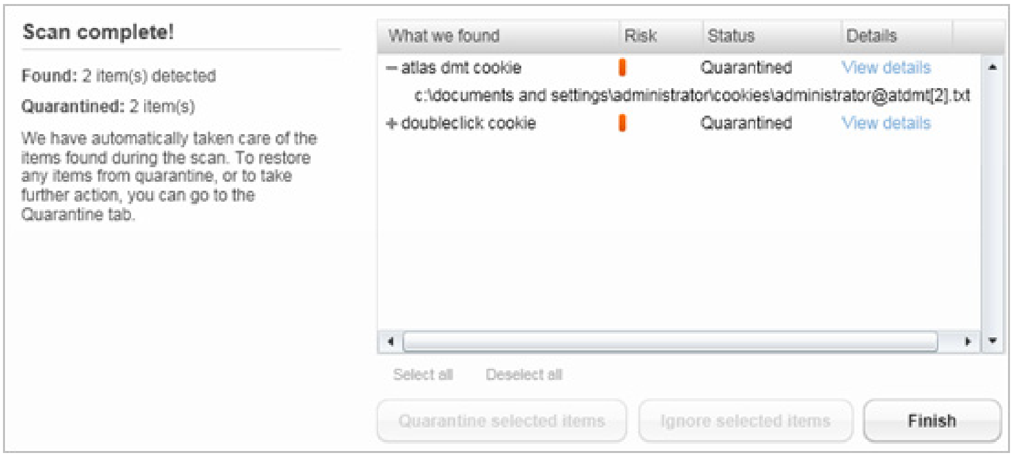
Automated scanning ON

The system is taking care of you.

Learn more about this

Schedule scans manually

Another panel opens and provides details about detected items.



Scan complete!

Found: 2 item(s) detected

Quarantined: 2 item(s)

We have automatically taken care of the items found during the scan. To restore any items from quarantine, or to take further action, you can go to the Quarantine tab.

What we found	Risk	Status	Details
– atlas dmt cookie	▮	Quarantined	View details
c:\documents and settings\administrator\cookies\administrator@atdmt[2].txt			
+ doubleclick cookie	▮	Quarantined	View details

Select all Deselect all

Quarantine selected items Ignore selected items Finish

See the following table for a description of the Scan Complete panel.

Scan details	
What we found	Name and description of the item. You can click the plus sign to the left of the item to view the directory where it was found.
Risk	The red-orange bars show the risk level of the selected item. Multiple bars indicate a higher risk, as follows: ▮ (low) ▮▮ (moderate) ▮▮▮ (high) ▮▮▮▮ (very high) ▮▮▮▮▮ (critical)

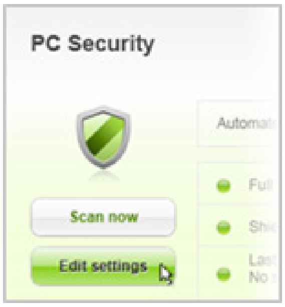
Scan details *(continued)*	
Status	This column shows how the System Scanner managed the item: • **Quarantined**. The item was moved to Quarantine, where it was rendered inoperable and cannot harm your computer. For more information, see Chapter 3, "Quarantine" on page 23. If you see a "Quarantined Error" status, contact Webroot Support. • **Suspect**. The item is classified as a "potentially unwanted application" and was not moved to Quarantine. You can decide to quarantine the item or keep it. If the scan launched while the main interface was closed, Webroot opens a notification that it completed the scan and found a potentially unwanted application. In this case, go to the Notifications panel to quarantine or keep the item. See "Responding to notifications" on page 10. • **Removed.** The item was deleted before the System Scanner quarantined it. This might happen if you are running another security program that removed it or if you manually deleted the file yourself during the scan. Any removed items are no longer a threat to your computer. • **Cleaned**. The item was managed by a virus-cleaning process that removed infected portions of the file and restored the cleaned file to your computer in its original location. A copy of the corrupted file is now in Quarantine. The cleaned file is safe to use; the file in Quarantine is not safe to use. In addition, the following status types can also appear if you managed an item yourself: • **Deleted**. You deleted the item from the Quarantine panel. See "Deleting quarantined items" on page 25. • **Restored**. You restored the item from the Quarantine panel. See "Restoring quarantined items" on page 26. • **Ignored**. You ignored a **"**Suspect**"** item in the Scan Complete panel. See "Scanning for threats" on page 14.
Details	If you don't recognize an item and want to know more about it, click **View details** to the right for a pop-up description.

Customizing scan options

You can change the scan settings to customize the locations where the System Scanner searches for threats and the types of threats it locates.

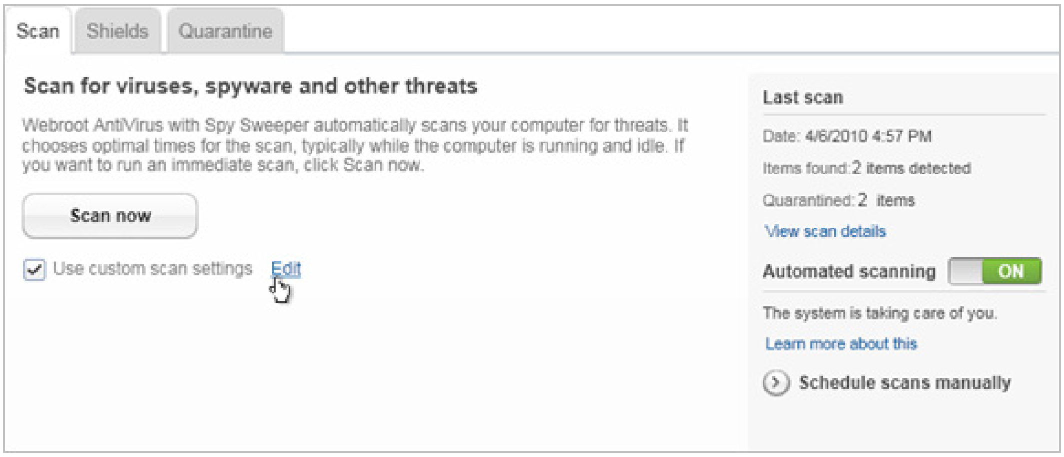
To customize scan settings:

1. Open the Webroot main interface by double-clicking the Webroot icon in the system tray.
2. From the Home panel, click the **Edit settings** button under PC Security.



The PC Security panel opens.

3. Make sure the **Scan** tab is selected.
4. Select the **Use custom scan settings** checkbox and click **Edit**.



Scan for viruses, spyware and other threats

Webroot AntiVirus with Spy Sweeper automatically scans your computer for threats. It chooses optimal times for the scan, typically while the computer is running and idle. If you want to run an immediate scan, click Scan now.

☑ Use custom scan settings

Last scan

Date: 4/6/2010 4:57 PM

Items found: 2 items detected

Quarantined: 2 items

View scan details

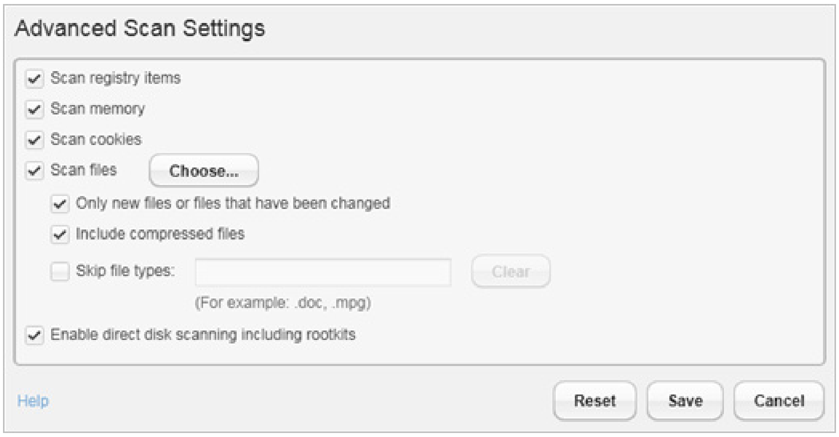
Automated scanning ON

The system is taking care of you.

Learn more about this

Schedule scans manually

The Advanced Scan Settings panel opens. Items with a checkmark are enabled and included in the next scan.



Advanced Scan Settings

☑ Scan registry items

☑ Scan memory

☑ Scan cookies

☑ Scan files

☑ Only new files or files that have been changed

☑ Include compressed files

□ Skip file types:

(For example: .doc, .mpg)

☑ Enable direct disk scanning including rootkits

5. Select or deselect options by clicking the checkboxes.

   The following table describes each setting.

6. When you’re done, click **Save**.

   The System Scanner uses these settings for all future scans.

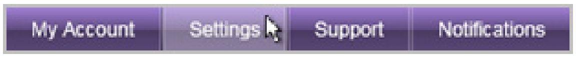
Advanced scan settings	
Scan registry items	Scans the computer’s registry, where spyware and other unwanted programs commonly create entries.
Scan memory	Scans the computer’s random access memory (RAM), where spyware and other unwanted programs commonly load into memory.
Scan cookies	Scans for third-party cookies that are included in the security definitions.
Scan files	Scans specific drives, directories, or files. Click the **Choose** button to open a pop-up dialog where you can specify areas to scan or ignore. Click in the checkboxes to deselect areas you don’t want to scan. Items with a checkmark are included in the scan; items without a checkmark are ignored. Click **OK** when you’re done.
Only new files or files that have been changed	Scans only the files that are new or modified from the last scan. Enabling this option decreases scan time significantly.
Include compressed files	Scans compressed files such as .zip, .rar, .lzh, and .cab files, where malware can hide. You may want to use this option after you have found spyware programs and you want to be sure that you have removed them. Enabling this option increases scan time significantly. (After the first scan with this option, the System Scanner skips compressed files that have not changed, thereby saving time.) If you download a compressed file in the future, you can scan just that file from Windows Explorer by right-clicking on the file and selecting **Perform Secure Scan** from the pop-up menu.
Skip file types	Scans specified file types only. Enter the extensions of file types you want the scan to ignore. For multiple entries, use a comma or semicolon to separate entries (for example: .mp3, .wma). Do not skip .dll, .exe, or .com file types, because malware typically hides in these types of files.
Enable direct disk scanning including rootkits	Scans for strains of spyware that hide themselves from the Windows operating system.

Creating a scan schedule

The System Scanner is preconfigured to run a scan at optimal times. If desired, you can disable automated scanning and set your own schedule.

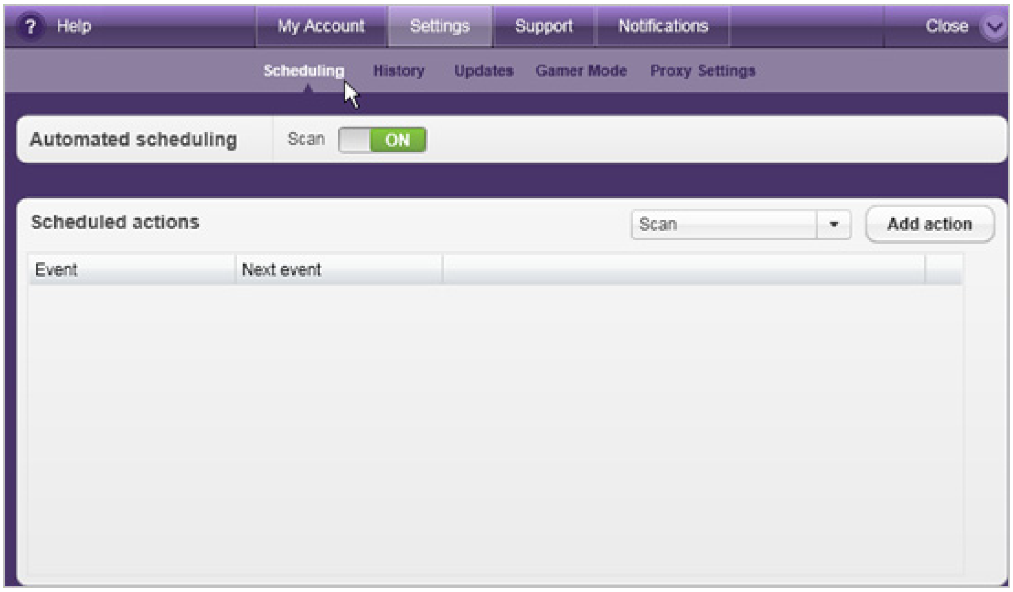
To create your own scan schedule:

1. Open the Webroot main interface by double-clicking the Webroot icon in the system tray.
2. From the bottom of the Home panel, click **Settings** in the taskbar.



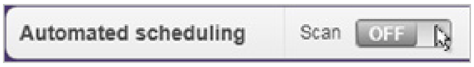
   The Settings panel opens.

3. Click **Scheduling**.



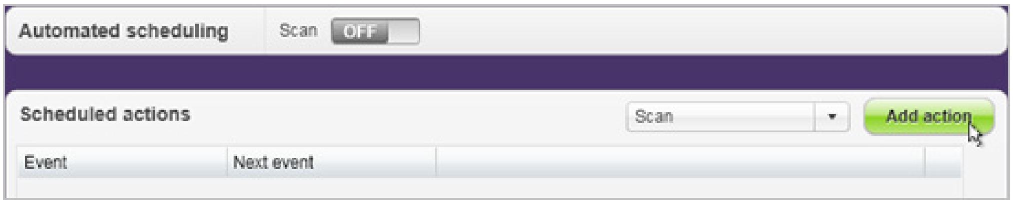
Automated scheduling Scan ON

4. Turn off scheduled scans by clicking the **ON/OFF** button, so the button changes to OFF.



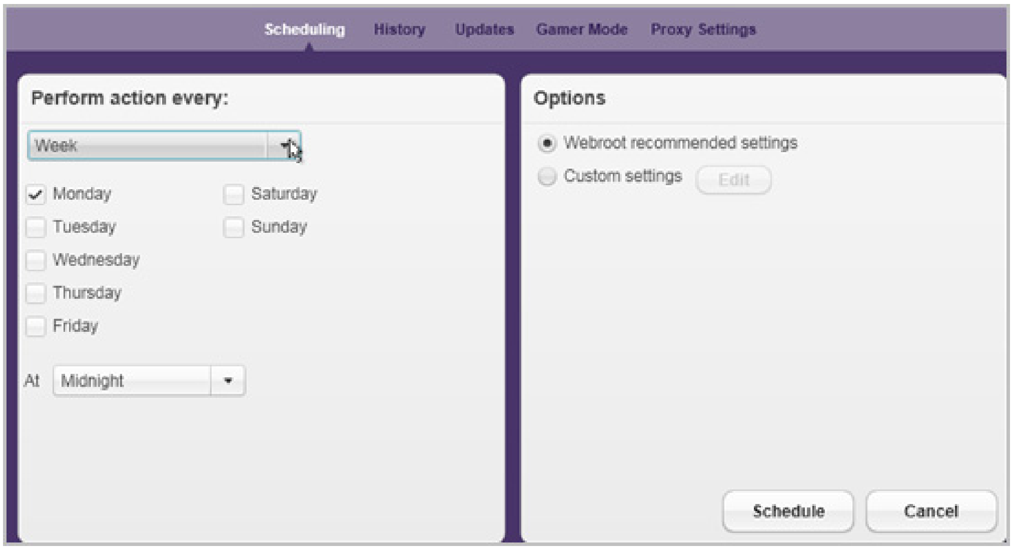
Automated scheduling Scan OFF

5. In the drop-down box, make sure **Scan** is displayed, then click the **Add action** button.



Automated scheduling Scan OFF

   The Scheduling panel opens.



Perform action every:

Week

☑ Monday
□ Tuesday
□ Wednesday
□ Thursday
□ Friday
□ Saturday
□ Sunday

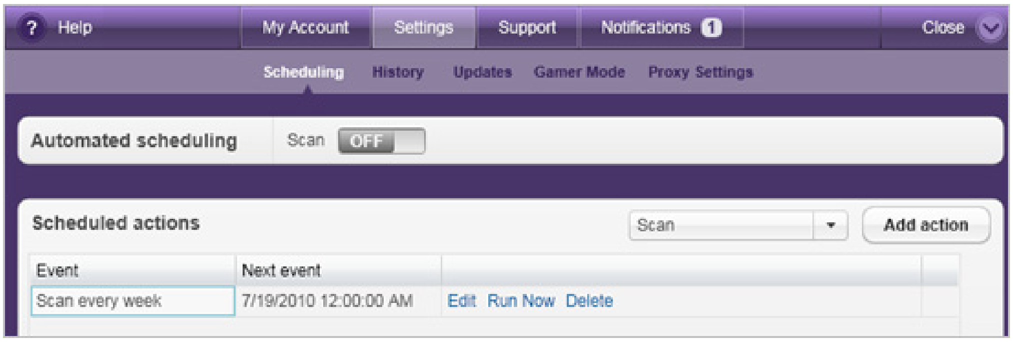
At Midnight

Options

● Webroot recommended settings
○ Custom settings Edit

6. Under **Perform action every**, determine the scan schedule as follows:
   - In the first field, click the drop-down arrow to select hour, day, week, month, or when you log in.
   - Click in the checkboxes to select one or more days of the week.
   - In the **At** field, click the drop-down arrow to select a time of day.
7. Under **Options**, you can select a radio button to keep the Webroot recommended settings or choose custom settings. For a description of the custom settings, see "Customizing scan options" on page 19.
8. Click the **Schedule** button.

   The panel shows details of your scheduled scan.



Automated scheduling Scan OFF

Scheduled actions Scan

Event	Next event	
Scan every week	7/19/2010 12:00:00 AM	Edit Run Now Delete

9. If desired, you can edit, delete, or run the schedules from the Scheduling panel by clicking either **Edit**, **Run Now**, or **Delete**.

3: Quarantine

The Webroot Quarantine is a holding area for potential threats. Items in Quarantine are rendered inoperable and cannot harm your computer.

In the quarantine process, the System Scanner removes all traces and items associated with threats from their current locations. It then disables their operation by scrambling and compressing all associated items, so the threats can no longer harm your computer or steal your information. Once the items are rendered inoperable, the System Scanner moves them to Quarantine. If the System Scanner detects a virus, it removes infected portions of a file during a virus cleaning process. If the System Scanner can remove the virus successfully, it restores the cleaned file to your computer in its original location and places a copy of the corrupted file in Quarantine. The cleaned file is safe to use; the file in Quarantine is not safe to use.

Once items are moved to Quarantine, your safest action is to simply keep them there. Items in Quarantine are disabled and cannot harm your computer. Keeping items in Quarantine also allows you to test your computer and determine if all your programs still work properly. If you discover that some legitimate programs cannot function after an item was moved to Quarantine, Webroot allows you to restore it.

To manage the Quarantine, see the following topics:

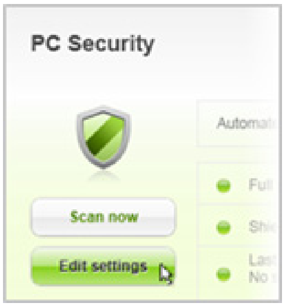
- "Viewing quarantined items" on page 24
- "Deleting quarantined items" on page 25
- "Restoring quarantined items" on page 26

Viewing quarantined items

Once items are quarantined, you can view more information about them in the Quarantine panel.

To view quarantined items:

1. Open the Webroot main interface by double-clicking the Webroot icon in the system tray.
2. From the Home panel, click the **Edit settings** button under PC Security.



The PC Security panel opens.

3. Click the **Quarantine** tab.

The Quarantine panel displays items that were previously detected during scans and moved to Quarantine.

You can select an item to see more details in the right pane. The following table describes the item details.

Item Details	
Name	Name of the item currently selected in the list.
Category	Type of item currently selected in the list. For more information about types of threats, see the "Glossary" on page 67.
Risk rating	The red-orange bars show the risk level of the selected item. The more bars shown, the higher the risk.
Description	Description of the item.

You can view more information about a selected item by clicking **View more details online**. (You must be connected to the Internet.)

Once items are stored in Quarantine, you can keep them there (the recommended action) or do one of the following:

- **Delete quarantined items permanently**. If the Quarantine area gets too full, Webroot alerts you to remove some items. You can permanently delete an item if you're sure it's unwanted spyware or another type of threat. For instructions, see the next section, "Deleting quarantined items."
- **Restore quarantined items**. If you discover that a legitimate program won't work properly when an item was moved to Quarantine, you can restore that item to its original location on the computer. For instructions, see "Restoring quarantined items" on page 26.

Deleting quarantined items

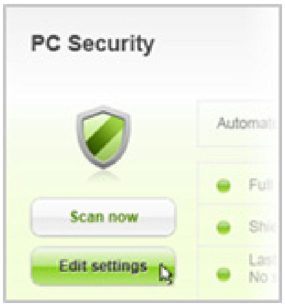
If desired, you can permanently delete items in Quarantine. Be aware that once you delete an item, it cannot be restored.

Note

Before deleting items in Quarantine, we recommend that you test your computer by opening and closing all your programs and performing a few tasks. In rare cases, programs classified as “spyware” may be an integral part of a legitimate application.

To permanently delete quarantined items:

1. Open the Webroot main interface by double-clicking the Webroot icon in the system tray.
2. From the Home panel, click the **Edit settings** button under PC Security.



The PC Security panel opens.

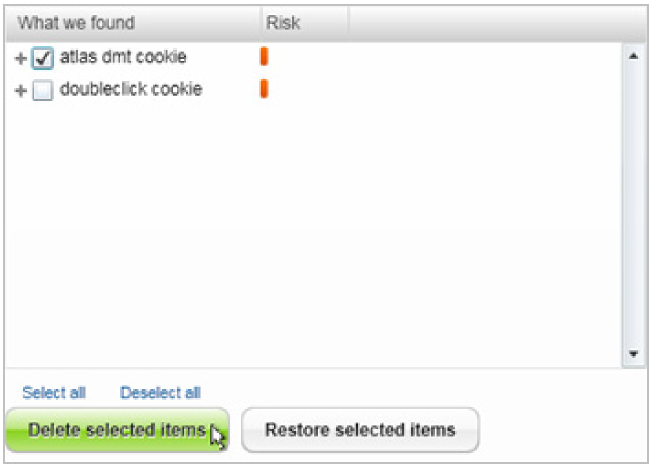
3. Click the **Quarantine** tab.

The Quarantine panel opens with a list of quarantined items.

4. Select each item that you want to permanently delete or click **Select All** at the bottom of the panel.

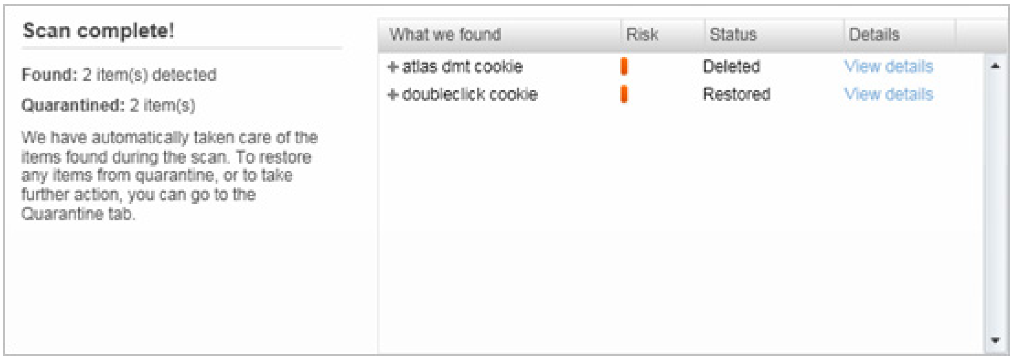
A checkmark next to the item shows that it is selected and will be deleted.

5. Click the **Delete selected items** button.



What we found	Risk
+ ☑ atlas dmt cookie	▮
+ □ doubleclick cookie	▮

The item is removed from the Quarantine panel. If you check the last scan details (see “Viewing scan details” on page 16), the item is still listed, but with “Deleted” as its status.



Scan complete!

Found: 2 item(s) detected

Quarantined: 2 item(s)

We have automatically taken care of the items found during the scan. To restore any items from quarantine, or to take further action, you can go to the Quarantine tab.

What we found	Risk	Status	Details
+ atlas dmt cookie	▮	Deleted	View details
+ doubleclick cookie	▮	Restored	View details

Restoring quarantined items

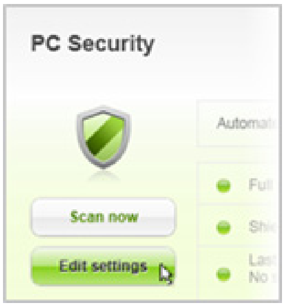
You may need to restore a quarantined item if you discover that a program is not working correctly without it. In rare cases, a piece of spyware is an integral part of a legitimate program and is required to run that program. (Some components with copy protection may not restore from Quarantine properly. You must reinstall these programs from the original media or installation file.)

Note

Never restore a file with a detected virus. If the Webroot software was able to clean the file (remove the virus safely), it keeps the cleaned file in its original location and places a copy of the corrupted file in Quarantine. The cleaned file is safe to use; the file in Quarantine is not safe to use.

To restore quarantined items:

1. Open the Webroot main interface by double-clicking the Webroot icon in the system tray.
2. From the Home panel, click the **Edit settings** button under PC Security.



The PC Security panel opens.

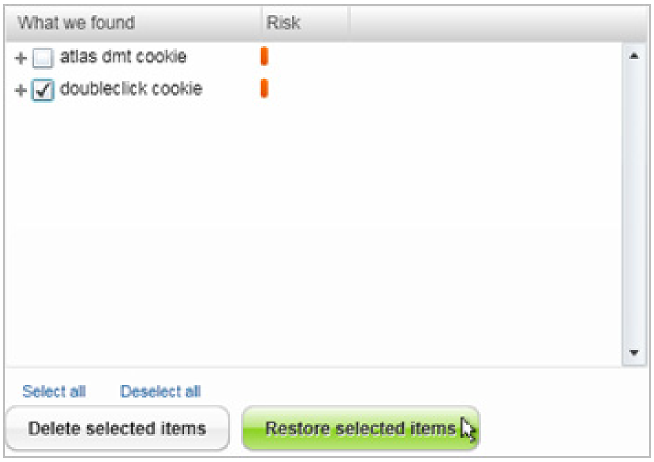
3. Click the **Quarantine** tab.

   The Quarantine panel opens with a list of quarantined items.

4. Select each item that you want to restore.

   A checkmark next to the item shows that it is selected and will be restored.

5. Click the **Restore selected items** button.



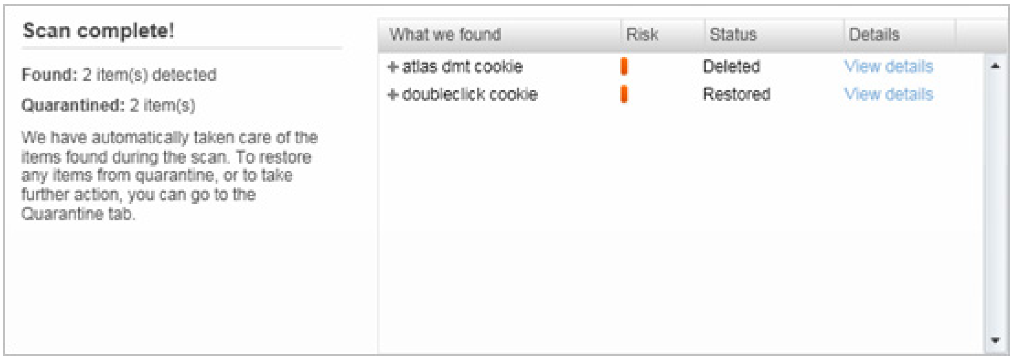
What we found	Risk
+ □ atlas dmt cookie	▮
+ ☑ doubleclick cookie	▮

The Webroot software restores the selected items to their original locations and shows the restore status at the bottom of the panel.

Note

If a selected item is part of an email attachment, the Webroot software saves it to the location specified in the **Always save to** option of the Email Attachments shield or prompts you to select the location to restore the attachment (if you selected the **Ask me where to save every file** option).

The item is removed from the Quarantine panel. If you check the last scan details (see "Viewing scan details" on page 16), the item is still listed, but with "Restored" as its status.



Scan complete!

Found: 2 item(s) detected

Quarantined: 2 item(s)

We have automatically taken care of the items found during the scan. To restore any items from quarantine, or to take further action, you can go to the Quarantine tab.

What we found	Risk	Status	Details
+ atlas dmt cookie	🟧	Deleted	View details
+ doubleclick cookie	🟧	Restored	View details

4: Shields

Webroot Shields monitor functions related to your Web browser settings, network communications between your computer and the Internet, Windows system settings, Windows Startup programs, and email attachments. If a suspicious item tries downloading or running on your computer, Webroot Shields automatically block and quarantine the item. For some types of shields, an alert asks if you want to continue the download or block it. If you don’t respond to the alert within one minute, Webroot Shields automatically block the download.

Webroot has already preconfigured the Webroot Shields for you, based on our recommended settings. You do not need to do anything. However, if you would like to modify the type of protection shields provide, you can change the settings as described in this chapter.

To manage shield settings, see the following topics:

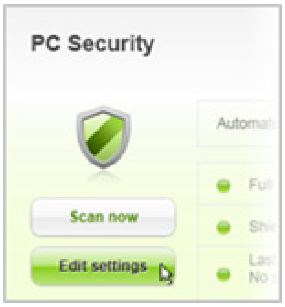
- “Setting real-time active protection” on page 30
- “Setting browser protection” on page 33
- “Setting network protection” on page 35

Setting real-time active protection

The Real-time Active Protection shields monitor your computer settings and activity. If these shields detect malware or viruses attempting to launch, they block these threats before they can damage your system.

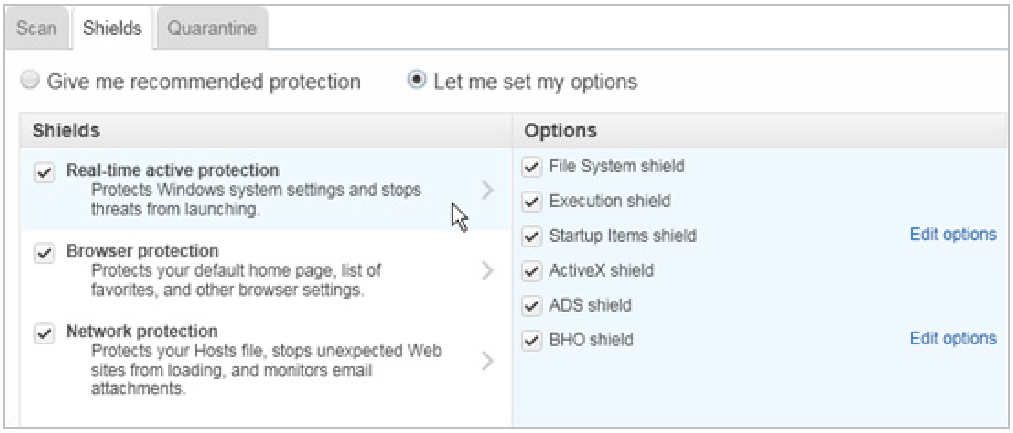
To set Real-time Active Protection shields:

1. Open the Webroot main interface by double-clicking the Webroot icon in the system tray.
2. From the Home panel, click the **Edit settings** button under PC Security.



   The PC Security panel opens.

3. Click the **Shields** tab.
4. Click **Let me set my options**.
5. Point your mouse to **Real-time active protection** and make sure the box to the left is checked.



Scan | Shields | Quarantine

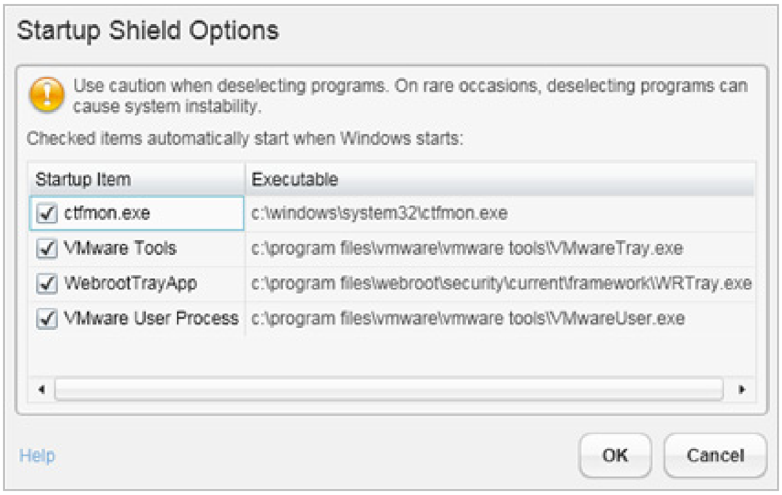
○ Give me recommended protection ● Let me set my options

Shields	Options
☑ Real-time active protection Protects Windows system settings and stops threats from launching.	☑ File System shield ☑ Execution shield ☑ Startup Items shield — Edit options ☑ ActiveX shield ☑ ADS shield ☑ BHO shield — Edit options
☑ Browser protection Protects your default home page, list of favorites, and other browser settings.	
☑ Network protection Protects your Hosts file, stops unexpected Web sites from loading, and monitors email attachments.	

   The Options pane displays the shield settings. Items with a checkmark are enabled.

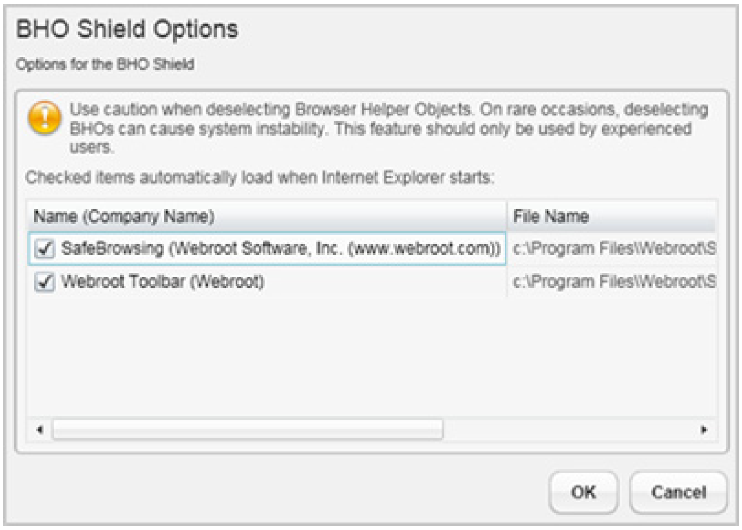
6. If you want to change a shield setting, select the checkbox next to the shield name to disable (uncheck) or activate (check) an option.

   The following table describes the function of each Real-time Active Protection shield.

<table>
<tr><th colspan="2">Real-time Active Protection shield options</th></tr>
<tr><td>File System shield</td><td>If this shield detects a threat attempting to launch during write and read operations, it sends the item to Quarantine.
<b>Note</b>: For read operations, the Webroot software can detect most, but not all file types.</td></tr>
<tr><td>Execution shield</td><td>If this shield detects a suspicious file trying to install or start, it sends the item to Quarantine.</td></tr>
<tr><td>Startup Items shield</td><td>If this shield detects malware or a virus attempting to add itself to the Windows startup list, it opens an alert where you can block or allow the file. (See “Responding to pop-up alerts” on page 8.)
If you want to change the list of programs that start with Windows, click <b>Edit options</b>.
The following dialog opens.


Startup Shield Options
Use caution when deselecting programs. On rare occasions, deselecting programs can cause system instability.
Checked items automatically start when Windows starts:
<table>
<tr><th>Startup Item</th><th>Executable</th></tr>
<tr><td>☑ ctfmon.exe</td><td>c:\windows\system32\ctfmon.exe</td></tr>
<tr><td>☑ VMware Tools</td><td>c:\program files\vmware\vmware tools\VMwareTray.exe</td></tr>
<tr><td>☑ WebrootTrayApp</td><td>c:\program files\webroot\security\current\framework\WRTray.exe</td></tr>
<tr><td>☑ VMware User Process</td><td>c:\program files\vmware\vmware tools\VMwareUser.exe</td></tr>
</table>

To see more information about a program, click the executable name. (Not all programs provide additional details.) If you do not want a program to start with Windows, deselect its checkbox and click <b>OK</b>.
<b><i>Caution</i></b>: Editing Startup Items is for advanced users. Windows and other programs may require some listed items, and if you remove them, your computer may not start properly.</td></tr>
<tr><td>ActiveX shield</td><td>If this shield detects ActiveX controls attempting to install on your computer, it opens an alert where you can block or allow the installation. (See “Responding to pop-up alerts” on page 8.)</td></tr>
<tr><td>ADS shield</td><td>If this shield detects programs or viruses that attempt to start from an Alternate Data Stream (ADS), it opens an alert where you can block or allow the installation.
(See “Responding to pop-up alerts” on page 8.)</td></tr>
</table>

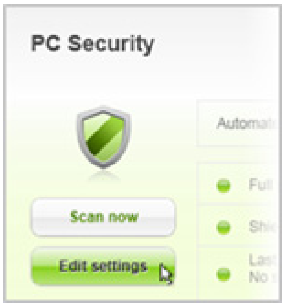
Real-time Active Protection shield options ***(continued)***	
BHO shield	If a Browser Helper Object (BHO) tries to install itself, it opens an alert where you can block or allow the installation. (See "Responding to pop-up alerts" on page 8.) If you want to change the BHOs that start with Internet Explorer, click **Edit options**. A dialog opens and shows a list of the installed BHOs. Items with a checkmark start whenever Internet Explorer starts. BHO Shield Options Options for the BHO Shield Use caution when deselecting Browser Helper Objects. On rare occasions, deselecting BHOs can cause system instability. This feature should only be used by experienced users. Checked items automatically load when Internet Explorer starts: Name (Company Name) — File Name ☑ SafeBrowsing (Webroot Software, Inc. (www.webroot.com)) — c:\Program Files\Webroot\S ☑ Webroot Toolbar (Webroot) — c:\Program Files\Webroot\S To see more information about an item, click the executable name. (Not all programs provide additional details.) Deselect any BHOs you do not want to start, then click **OK**. ***Caution***: Editing BHOs is for advanced users. Deselecting BHOs could cause your browser to not work properly or cause your computer to be unstable. Do *not* attempt to disable the Webroot toolbar. This may result in unexpected behavior and will disable access to some Webroot software functionality.

Setting browser protection

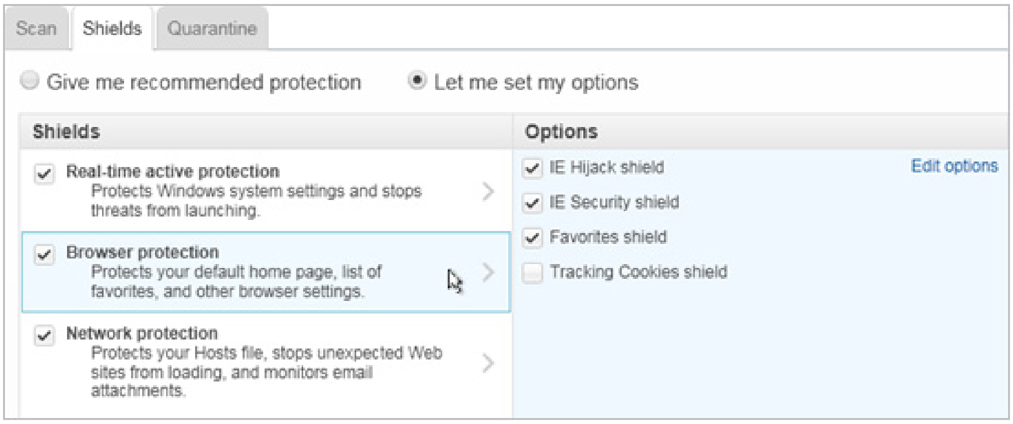
Browser Protection shields guard your default Home page, list of favorites, and other settings related to your Web browser.

To set Browser Protection shields:

1. Open the Webroot main interface by double-clicking the Webroot icon in the system tray.
2. From the Home panel, click the **Edit settings** button under PC Security.

   The PC Security panel opens.
3. Click the **Shields** tab.
4. Click **Let me set my options**.
5. Point your mouse to Browser protection and make sure the box to the left is checked.

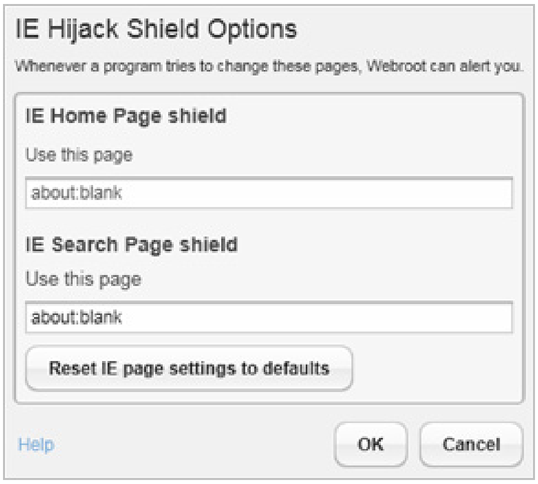
   Scan | Shields | Quarantine

   ○ Give me recommended protection ● Let me set my options

Shields	Options
☑ Real-time active protection Protects Windows system settings and stops threats from launching.	☑ IE Hijack shield ☑ IE Security shield ☑ Favorites shield □ Tracking Cookies shield
☑ Browser protection Protects your default home page, list of favorites, and other browser settings.	
☑ Network protection Protects your Hosts file, stops unexpected Web sites from loading, and monitors email attachments.	

   The Options pane displays the shield settings. Items with a checkmark are enabled.
6. If you want to change a shield setting, select the checkbox next to the shield name to disable (uncheck) or activate (check) an option.

   The following table describes the function of each Browser Protection shield.

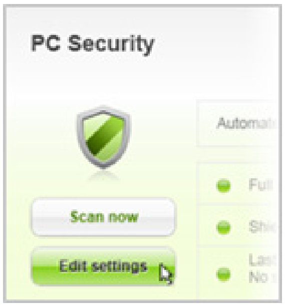
Browser Protection shield options	
IE Hijack shield	If this shield detects a spyware program trying to change the default pages that open in Internet Explorer, such as your set Home page, it opens an alert where you can allow or block the change. To check or change the default pages for Internet Explorer, click **Edit options**. The following dialog opens.  IE Hijack Shield Options Whenever a program tries to change these pages, Webroot can alert you. IE Home Page shield Use this page about:blank IE Search Page shield Use this page about:blank You can edit the following addresses: • **IE Home Page shield**: In the field, you can enter a new Web site address for your Home page. The address must be in the following format: http://www.webroot.com. • **IE Search Page shield**: In the field, you can enter a new Web address for the informational page that opens when you attempt to access a non-existent Web site. The address must be in the following format: http://www.microsoft.com. If you want to return to the Internet Explorer default pages, select the **Reset IE page settings to defaults** button.
IE Security shield	If a program tries to change your Internet Explorer security settings, this shield opens an alert where you can allow or block the change.
Favorites shield	If a spyware program tries to change your Internet Explorer or Firefox list of favorite Web sites, this shield opens an alert where you can allow or block the change.
Tracking Cookies shield	If third-party cookies attempt to download to your computer, this shield blocks them.

Setting network protection

Network Protection shields guard your Hosts file, stop unexpected Web sites from loading, and monitor email attachments.

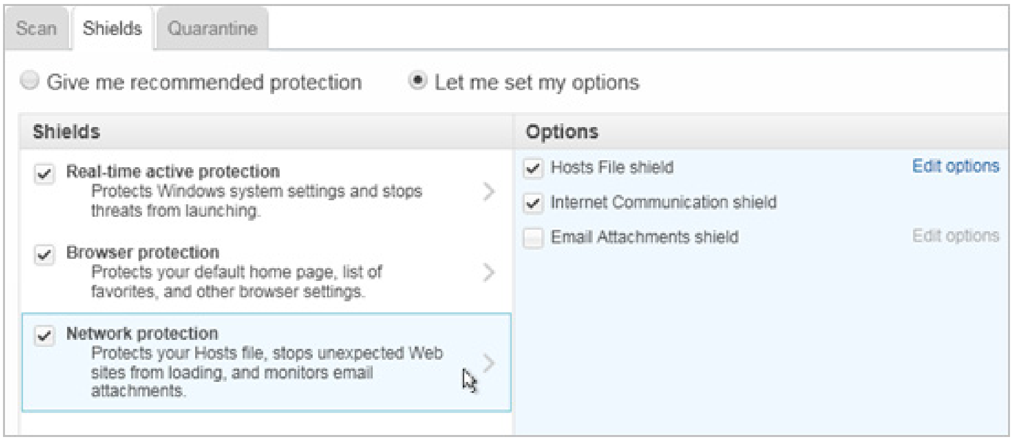
To set Network Protection shields:

1. Open the Webroot main interface by double-clicking the Webroot icon in the system tray.
2. From the Home panel, click the **Edit settings** button under PC Security.



The PC Security panel opens.

3. Click the **Shields** tab.
4. Click **Let me set my options**.
5. Point your mouse to **Network protection** and make sure the box to the left is checked.



○ Give me recommended protection ● Let me set my options

Shields

☑ Real-time active protection
Protects Windows system settings and stops threats from launching.

☑ Browser protection
Protects your default home page, list of favorites, and other browser settings.

☑ Network protection
Protects your Hosts file, stops unexpected Web sites from loading, and monitors email attachments.

Options

☑ Hosts File shield

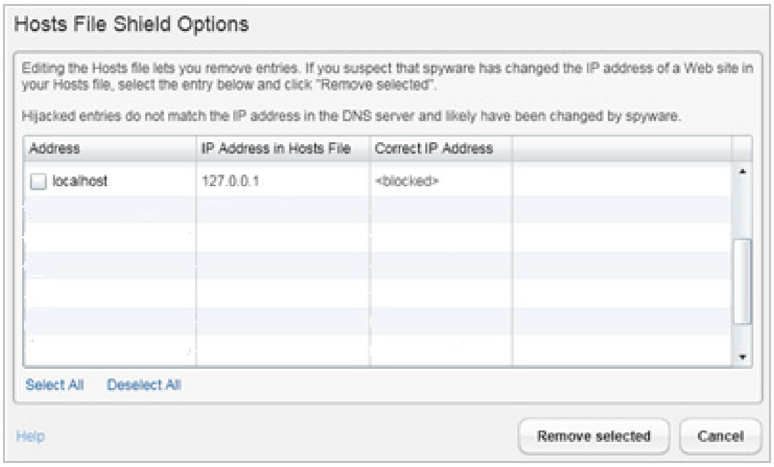
☑ Internet Communication shield

□ Email Attachments shield

The Options pane displays the shield settings. Items with a checkmark are enabled.

6. If you want to change a shield setting, select the checkbox next to the shield name to disable (uncheck) or activate (check) an option.

The following table describes the function of each Network Protection shield.

Network Protection shield options	
Hosts File shield	If this shield detects spyware programs attempting to add or change the IP address for a Web site in the Hosts file, it opens an alert where you can block or allow the changes. (See “Responding to pop-up alerts” on page 8.) The Hosts file is a Windows file that helps direct your computer to a Web site using Internet Protocol (IP) addresses. Your Web browser uses the IP address to actually connect to a site. When you enter a Web address in a browser, your computer first looks in the Hosts file to see if it already knows where to go. If the domain is listed (for example, webroot.com), your computer goes directly to the IP address. If the domain is not listed, your computer looks up the information from the Internet, which is a slightly slower process. If you suspect that spyware tampered with the entries in your Hosts file, click **Edit options**. The Hosts File Shield Options dialog shows entries that you, your IT department, or potential spyware programs have added to your Hosts file.  Hosts File Shield Options Editing the Hosts file lets you remove entries. If you suspect that spyware has changed the IP address of a Web site in your Hosts file, select the entry below and click "Remove selected". Hijacked entries do not match the IP address in the DNS server and likely have been changed by spyware. Address IP Address in Hosts File Correct IP Address □ localhost 127.0.0.1 <blocked> Select All Deselect All Help Remove selected Cancel If any entries appear to be spyware related, select the checkbox next to the address and click **Remove selected**. If you aren’t sure whether the entries are valid, contact Webroot Support. ***Caution***: Editing the Hosts file is for advanced users.
Internet Communication shield	This shield monitors communication from your computer to known Web sites that are related to spyware or potential threats. Webroot includes a list of known sites with its security definitions. If the shield detects an attempt to communicate with a site on the list, it opens an alert. (See “Responding to pop-up alerts” on page 8.)

Network Protection shield options *(continued)*

Email Attachments shield

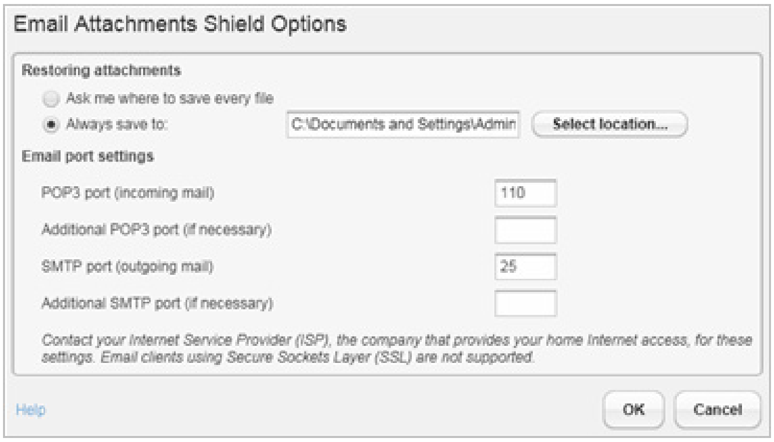
(*Does not support email clients that use SSL*)

This shield monitors file attachments for incoming email (through POP3 protocol) and outgoing email (through SMTP protocol). If it detects that an attachment or its contents match a security definition, it replaces the content of the attachment with an alert message that describes what it found. This shield then moves the original attachment to Quarantine, where you can decide whether to save it to your computer or delete it. You can also direct the shield to always restore quarantined email attachments to a specific directory.

By default, Webroot monitors port 110 (POP3) for incoming mail and port 25 (SMTP) for outgoing mail, but you can change the port numbers in the Email Attachments settings, if necessary.

Note: Some firewall configurations might prevent the Email Attachments shield from monitoring email. For more information, see the note on page 38.

For Email Attachments Shield options, click **Edit options**. The following dialog opens:



Email Attachments Shield Options

Restoring attachments

○ Ask me where to save every file

● Always save to: C:\Documents and Settings\Admin

Email port settings

POP3 port (incoming mail)	110
Additional POP3 port (if necessary)	
SMTP port (outgoing mail)	25
Additional SMTP port (if necessary)	

Contact your Internet Service Provider (ISP), the company that provides your home Internet access, for these settings. Email clients using Secure Sockets Layer (SSL) are not supported.

Set the options as follows:

- **Restoring attachments**: Select **Ask me where to save every file** if you want to be prompted when it restores quarantined attachments. Select **Always save to** if you want to create a default location for restored email attachments. You can enter a file location in the field or click **Select location** to browse directories from Windows Explorer.
- **Email port settings**: Enter the POP3 port number for incoming mail and the SMTP port number for outgoing mail. This dialog automatically displays port numbers that most computers use for email communications. If necessary, change the port numbers or contact your ISP (Internet Service Provider) for the port numbers.

Note

Communication errors with the Email Attachments shield:
Some firewall applications from other vendors might prevent the Webroot software from intercepting email traffic. If this is the case, Webroot opens an alert every time an email is sent or received. If an alert appears because a firewall application is blocking the Webroot software, you need to configure your firewall application to allow the program to monitor the port traffic. For more information about resolving communication issues between your firewall application and the Webroot software, you can contact Webroot Support or enter the following address into your browser for instructions:

```
http://www.webroot.com/land/
personal_firewall_config.php?pc=64150&rc=1&oc=110&mjv=5&mnv=5&la
ng=en&loc=USA&opi=2&omj=5&omn=1
```

If the alert appears only once or just periodically, the problem may be due to an inactive network configuration or a non-responsive SMTP or POP server at the ISP (Internet Service Provider). This is a temporary situation. The Email Attachments shield should be able to function normally once communication is restored. If the message appears frequently when these types of communication errors occur, you can select **Do not show this message again**.

5: My Account Management

Your Webroot account allows you to access some helpful information about your software licenses and other details. Your account information is available from *My Webroot*, an online Web area that is accessible at any time. For more information, see "Using My Webroot" on page 11.

If you have not created an account, see "Creating a Webroot account" on page 2.

To manage your Webroot account, see the following topics:

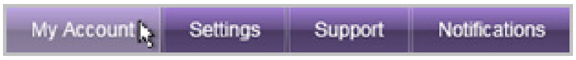
- "Viewing account details" on page 40
- "Editing your contact information and password" on page 41
- "Managing licenses and additional products" on page 42
- "Creating Webroot support tickets" on page 43

Viewing account details

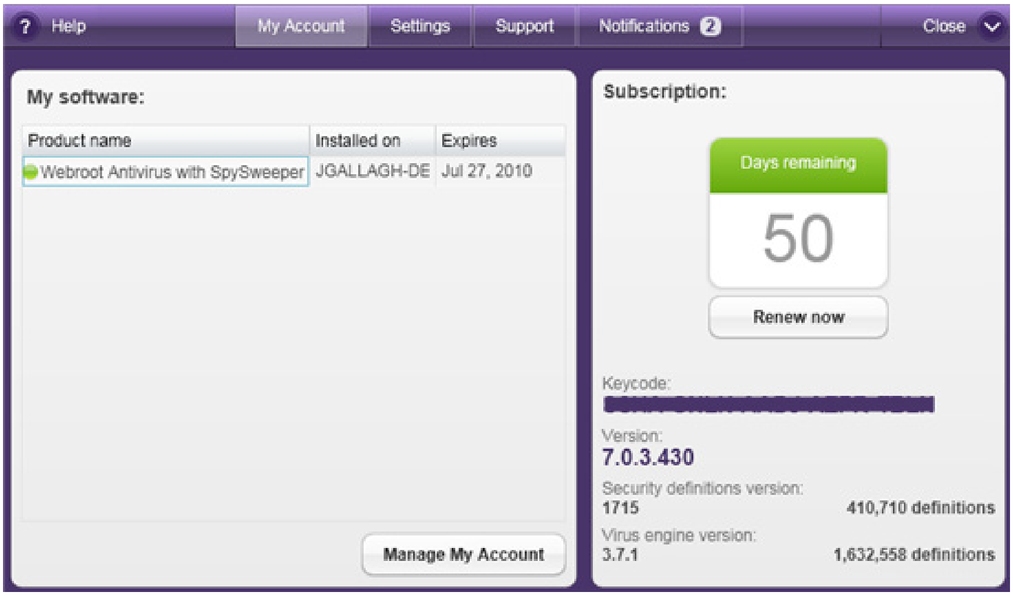
Your account details are available from the My Account panel in the main interface and in *My Webroot*. These details show your expiration date and your keycode.

To view account details from the main interface:

1. Open the Webroot main interface by double-clicking the Webroot icon in the system tray.
2. From the taskbar at bottom of the Home panel, click **My Account**.



The My Account panel opens and shows your keycode, version number, and other information about your subscription.



My software:

Product name	Installed on	Expires
Webroot Antivirus with SpySweeper	JGALLAGH-DE	Jul 27, 2010

Subscription:

Days remaining
50

Keycode:
[redacted]

Version:
7.0.3.430

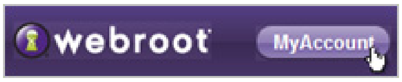
Security definitions version:
1715 410,710 definitions

Virus engine version:
3.7.1 1,632,558 definitions

3. To modify account details from *My Webroot*, click the **Manage My Account** button.

To view account details from *My Webroot*:

1. Open your browser and enter https://www.webroot.com/mywebroot. In the Sign In panel, enter your user name (email address) and password, then click the **Sign in** button.
2. When *My Webroot* opens with your account information, select **MyAccount** from the top panel.



The MyAccount page opens. It includes all your account information and available tasks. For more information, see the following sections:

- "Editing your contact information and password" on page 41
- "Managing licenses and additional products" on page 42
- "Creating Webroot support tickets" on page 43

Editing your contact information and password

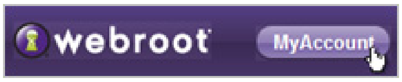
From the Contact Information tab, you can enter or change your personal contact information so Webroot can contact you for product update announcements. You can also change your Webroot master password from this tab.

Note

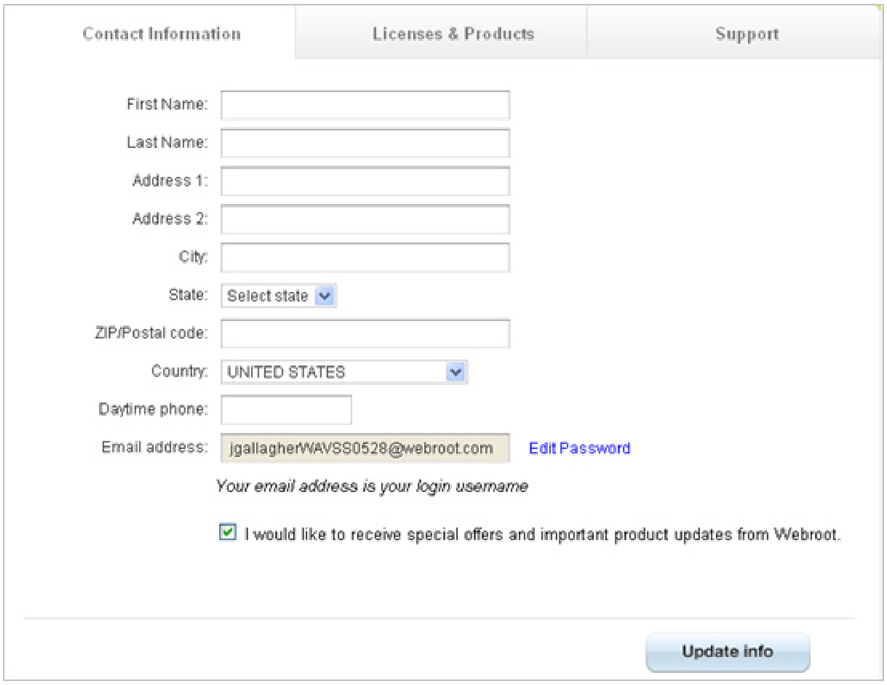
If you cannot remember your account password, open the Sign in screen and click **Forgot Your Password?**. In the dialog that opens, enter your email address and click **Send Email**. Webroot sends a message to your email address with instructions for resetting your password.

To edit contact information or change your password:

1. Open your browser and enter https://www.webroot.com/mywebroot. In the Sign In panel, enter your user name (email address) and password, then click the **Sign in** button. (If you are already signed in, this button displays **Sign Out**.)
2. When *My Webroot* opens with your account information, select **MyAccount** from the top panel.



3. Click the **Contact Information** tab.
4. Enter your personal information in the fields. If you want to change your password, click the **Edit Password** link and follow the on-screen instructions.
5. When you're done, click **Update info**.



First Name:

Last Name:

Address 1:

Address 2:

City:

State: Select state

ZIP/Postal code:

Country: UNITED STATES

Daytime phone:

Email address: jgallagherWAVSS0528@webroot.com Edit Password

Your email address is your login username

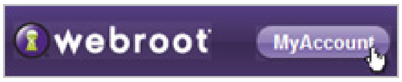
☑ I would like to receive special offers and important product updates from Webroot.

Managing licenses and additional products

You can view your Webroot license information for the status of any Webroot products you have purchased. The license information includes the product name, the keycode, where the software is installed (which computer), and when your subscription expires. You can also use this page to re-install your licensed software, install it onto another computer, or renew your subscription.

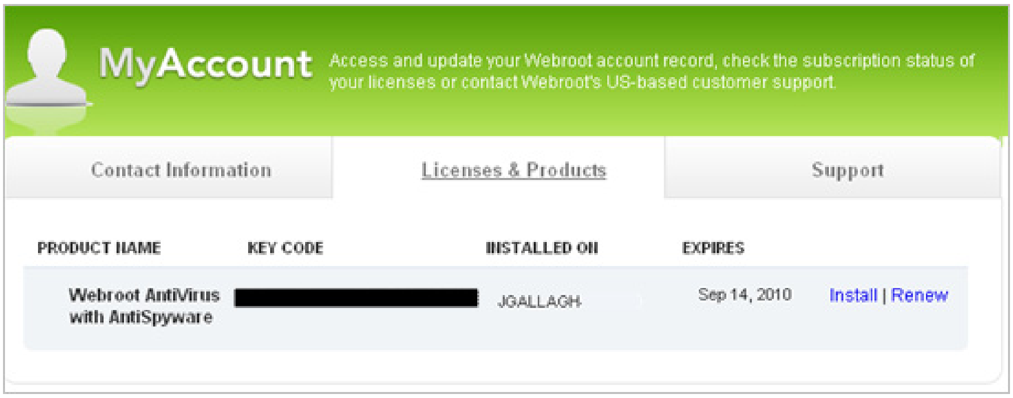
To view your current licenses and upgrade your Webroot products:

1. Open your browser and enter https://www.webroot.com/mywebroot. In the Sign In panel, enter your user name (email address) and password, then click the **Sign in** button. (If you are already signed in, this button displays **Sign Out**.)
2. When *My Webroot* opens with your account information, select **MyAccount** from the top panel.



3. Click the **Licenses & Products** tab.

   Your license information opens, similar to the example below.



MyAccount Access and update your Webroot account record, check the subscription status of your licenses or contact Webroot's US-based customer support.

PRODUCT NAME	KEY CODE	INSTALLED ON	EXPIRES	
Webroot AntiVirus with AntiSpyware	[redacted]	JGALLAGH	Sep 14, 2010	Install | Renew

From this page, you can:

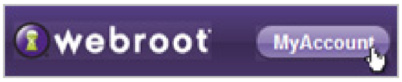
- Click **Install** to re-install your software or install it onto another computer if you have a multi-licensed version.
- Click **Renew** to update your subscription.

Creating Webroot support tickets

If you have questions or problems, you can create a support ticket to send to Webroot or view past tickets.

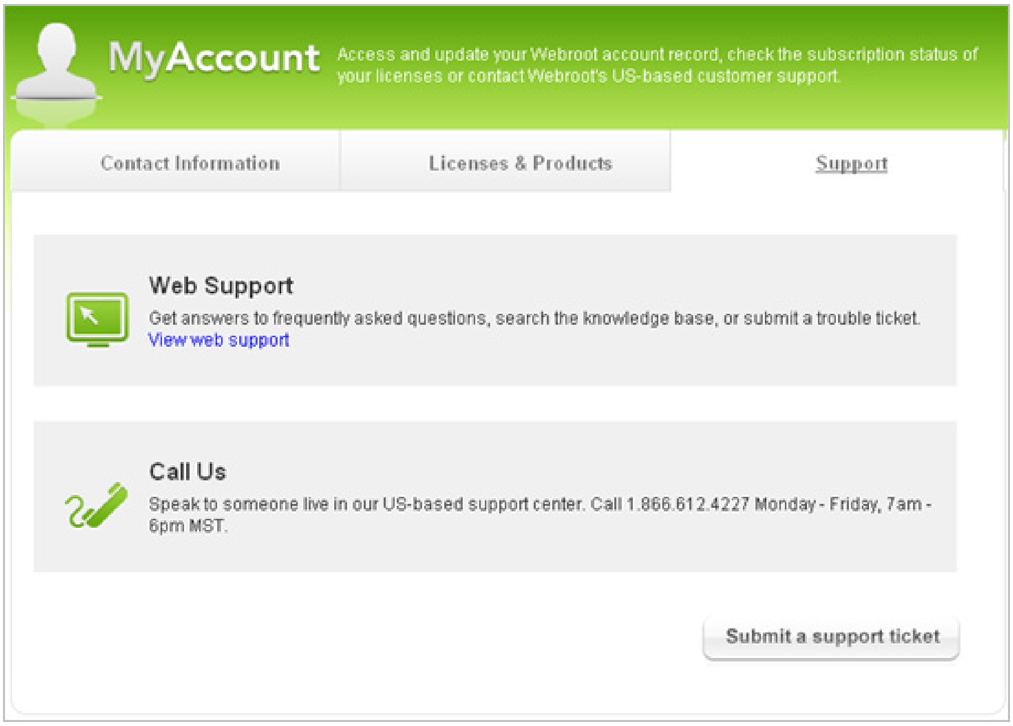
To create a support ticket:

1. Open your browser and enter https://www.webroot.com/mywebroot. In the Sign In panel, enter your user name (email address) and password, then click the **Sign in** button. (If you are already signed in, this button displays **Sign Out**.)
2. When *My Webroot* opens with your account information, select **MyAccount** from the top panel.



   Your Webroot account information opens.

3. Click the **Support** tab.



Access and update your Webroot account record, check the subscription status of your licenses or contact Webroot's US-based customer support.

Web Support

Get answers to frequently asked questions, search the knowledge base, or submit a trouble ticket.

View web support

Call Us

Speak to someone live in our US-based support center. Call 1.866.612.4227 Monday - Friday, 7am - 6pm MST.

4. If you would like to contact Support via email, click the **Submit a support ticket** button. A form opens in your browser that you can fill out and submit to Webroot.

6: Program Settings

The Webroot software includes options that allow you to control sweep schedules, view history logs, and other items related to program activity.

To manage program settings, see the following topics:

- "Managing the schedule for scans" on page 46
- "Viewing the system history" on page 47
- "Managing updates" on page 48
- "Setting Gamer mode" on page 50
- "Using a proxy server" on page 52

Managing the schedule for scans

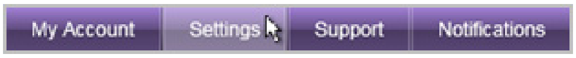
If you have previously created a schedule for scans, you can edit, delete, or run the schedules from the Scheduling panel.

Note

To create a schedule for scans, see "Creating a scan schedule" on page 21.

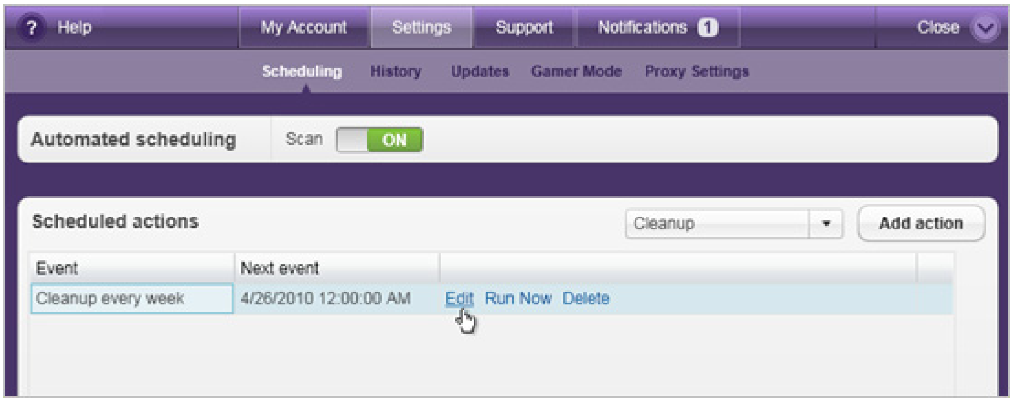
To manage schedules:

1. Open the Webroot main interface by double-clicking the Webroot icon in the system tray.
2. From the taskbar at the bottom of the Home panel, click **Settings**.



   The Settings panel opens.

3. Click **Scheduling**.
4. In the row for your scheduled event, click either **Edit**, **Run Now**, or **Delete**.



Automated scheduling — Scan: ON

Scheduled actions — Cleanup

Event	Next event	
Cleanup every week	4/26/2010 12:00:00 AM	Edit Run Now Delete

5. Click the **Close** button at the top right to close the panel.

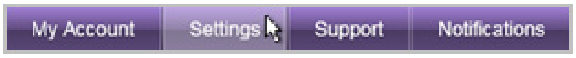
Viewing the system history

The History panel displays past Webroot software actions, such as:

- Scans (automated, scheduled, and manual)
- Quarantine actions
- Individual shield events
- Definition updates
- Product updates

To view the detection history:

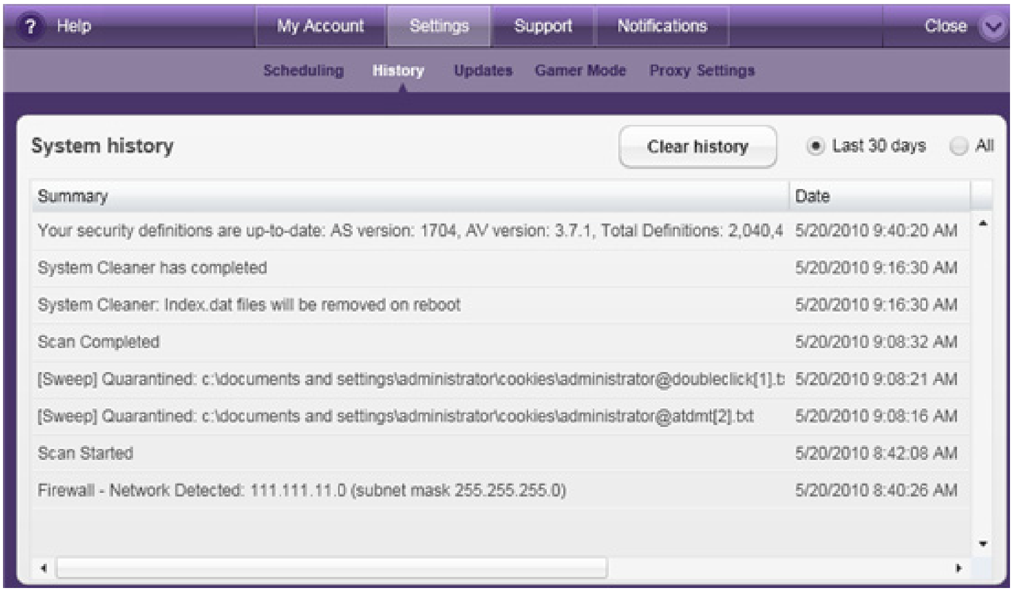
1. Open the Webroot main interface by double-clicking the Webroot icon in the system tray.
2. From the taskbar at the bottom of the Home panel, click **Settings**.



The Settings panel opens.

3. Click **History**.

The System History panel shows a summary of events and the dates on which they occurred, similar to the example below.



System history

Summary	Date
Your security definitions are up-to-date: AS version: 1704, AV version: 3.7.1, Total Definitions: 2,040,4	5/20/2010 9:40:20 AM
System Cleaner has completed	5/20/2010 9:16:30 AM
System Cleaner: Index.dat files will be removed on reboot	5/20/2010 9:16:30 AM
Scan Completed	5/20/2010 9:08:32 AM
[Sweep] Quarantined: c:\documents and settings\administrator\cookies\administrator@doubleclick[1].t	5/20/2010 9:08:21 AM
[Sweep] Quarantined: c:\documents and settings\administrator\cookies\administrator@atdmt[2].txt	5/20/2010 9:08:16 AM
Scan Started	5/20/2010 8:42:08 AM
Firewall - Network Detected: 111.111.11.0 (subnet mask 255.255.255.0)	5/20/2010 8:40:26 AM

4. To display all activity, click the **All** radio button. To display only the activity for the last 30 days, click the **Last 30 Days** radio button.
5. To clear the contents of this panel, click the **Clear history** button.
6. Click the **Close** button at the top right to close the panel.

Managing updates

The Webroot software is preconfigured to check for updates once a day. When available, the following items download during updates:

- Product updates, which include new versions of the Webroot program.
- Protection updates, which include the latest security definitions used to determine if any items found on your computer match spyware, viruses, or other threats.

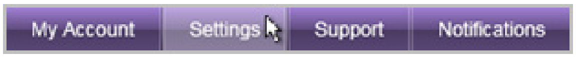
You must be connected to the Internet for update checks to be successful.

Note

Microsoft Silverlight is installed along with your Webroot software. On occasion, you may receive notifications from Microsoft about updating Silverlight.

To check for updates immediately or to change settings for automatic updates:

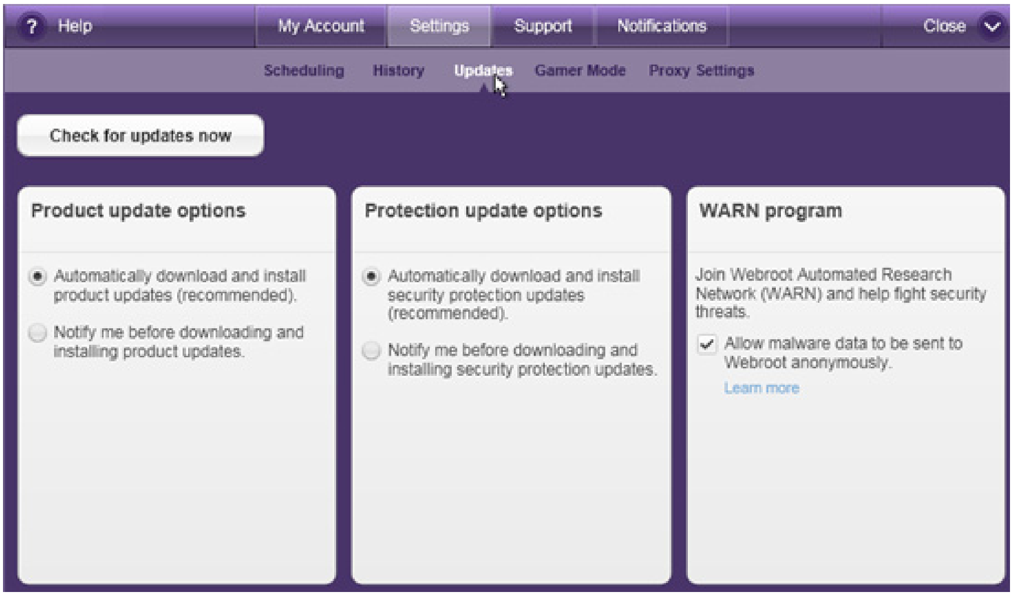
1. Open the Webroot main interface by double-clicking the Webroot icon in the system tray.
2. From the taskbar at the bottom of the Home panel, click **Settings**.



   The Settings panel opens.

3. Click **Updates**.

   The Updates panel opens.



Product update options

● Automatically download and install product updates (recommended).

○ Notify me before downloading and installing product updates.

Protection update options

● Automatically download and install security protection updates (recommended).

○ Notify me before downloading and installing security protection updates.

WARN program

Join Webroot Automated Research Network (WARN) and help fight security threats.

☑ Allow malware data to be sent to Webroot anonymously.

Learn more

4. You can click the **Check for updates now** button to download and install any available updates immediately or you can change the selections for automatic updates, which are described in the following table. To change an option, click the radio button next to the selection.

Product update options	
Automatically download and install product updates (recommended)	If selected, updates to the Webroot software download and install to your computer automatically (if available) when your computer is connected to the Internet.
Notify me before downloading and installing product updates	If selected, updates do *not* download and install to your computer automatically. Instead, a notification panel opens and allows you to determine if you want to download and install updates to the Webroot software (when available).
Protection update options	
Automatically download and install security protection updates (recommended)	If selected, updates to the security definitions download and install to your computer automatically (if available) when your computer is connected to the Internet.
Notify me before downloading and installing security protection updates	If selected, updates do *not* download and install to your computer automatically. Instead, a notification panel opens and allows you to determine if you want to download and install updates to the security definitions (when available).
WARN (Webroot Automated Research Network) program	
Allow malware data to be sent to Webroot anonymously	If selected, allows the software to gather information during scans and shielding activities, including spyware, viruses, and potential threats that are not yet classified, then send the data to Webroot. WARN is a global community of individuals and businesses who provide Webroot with sample items detected on their computer to help us identify and fight emerging threats. **Note:** The Webroot software does not gather personal information with the WARN program.

Setting Gamer mode

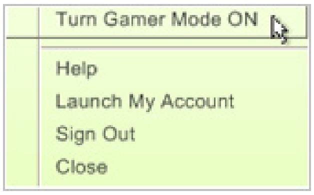
If the Webroot software's communications over the Internet interfere when you play online games or view movies, you can set the program to a silent Gamer mode. While in this mode, the program does not perform the following activities:

- Scheduled scans. The software does not run scheduled scans when Gamer mode is on. When you return the Webroot software to regular operations (Gamer mode is switched off), it may open an alert that indicates a scheduled scan was missed. The missed event does not run automatically.
- Shield functions. All shields will be turned off, except for the Execution shield, which stops executable programs from launching a suspicious process on your computer. If the Execution shield detects a potential threat, it moves the item to Quarantine without alerting you.
- Balloon alerts in the system tray.
- Communications with the Webroot server to check for updates.

To set Gamer mode:

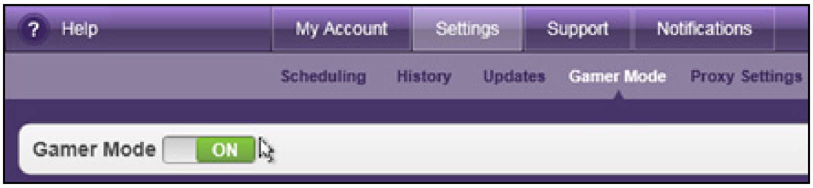
Do either of the following:

- From the system tray, right-click on the Webroot icon and select **Turn Gamer Mode ON**.

  - or -

- From the main interface, click **Settings** in the bottom taskbar, click the **Gamer Mode** tab, then click the button next to **Gamer Mode** so it displays "ON."

  By default, Gamer mode automatically turns off after four hours, but you can change that amount of time in the Options settings.

To manually turn off Gamer mode:

Do either of the following:

- From the system tray, right-click on the Webroot icon and select **Turn Gamer Mode OFF**.

  - or -

- From the main interface, click **Settings** in the bottom taskbar, click the **Gamer Mode** tab, then click the button next to **Gamer Mode** so it displays "OFF."

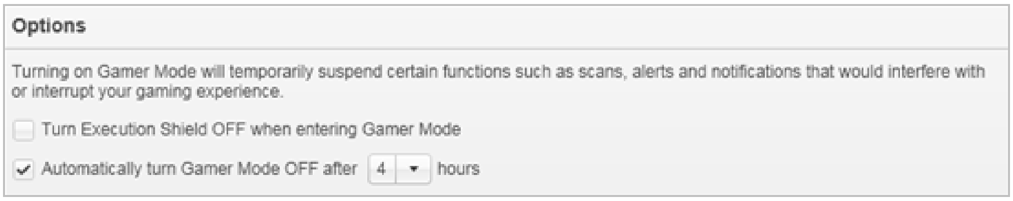
  All program activities are re-enabled, including the previously set shields. The Webroot software also contacts the Webroot server and checks for any updates.

> **Note**
>
> If you shut down and restart the Webroot software, it disables Gamer mode on start-up.

To change Gamer mode options:

1. From the main interface, click **Settings** in the bottom taskbar, then click **Gamer Mode**.

   The Gamer mode options appear in the middle panel.



Options

Turning on Gamer Mode will temporarily suspend certain functions such as scans, alerts and notifications that would interfere with or interrupt your gaming experience.

□ Turn Execution Shield OFF when entering Gamer Mode

☑ Automatically turn Gamer Mode OFF after 4 ▾ hours

   You can set the following options:

   - **Turn Execution Shield OFF when entering Gamer Mode**. When you set the program to Gamer mode, all shields are turned off except for the Execution shield. (The Execution shield is important because it can stop potentially harmful executable files from launching on your computer.) If desired, you can specify that the Execution shield is turned off along with all other shields.

   - **Automatically turn Gamer Mode OFF after ...** You can specify how long you want to run the program in Gamer mode before it automatically switches back to regular operations.

2. Enter the number of hours you want to use Gamer mode before it turns off and switches to regular program operations. If you do not want Gamer mode to automatically switch off, deselect the checkbox.

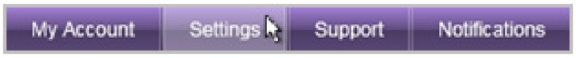
Using a proxy server

If you use a proxy server to connect to the Internet, you must specify information about the proxy connection; otherwise, Webroot cannot send updates to your computer. (A *proxy server* is a computer system or router that acts as a relay between your computer and another server.)

By default, the Webroot software is set to communicate directly with your computer (and not use a proxy server).

To specify proxy server settings:

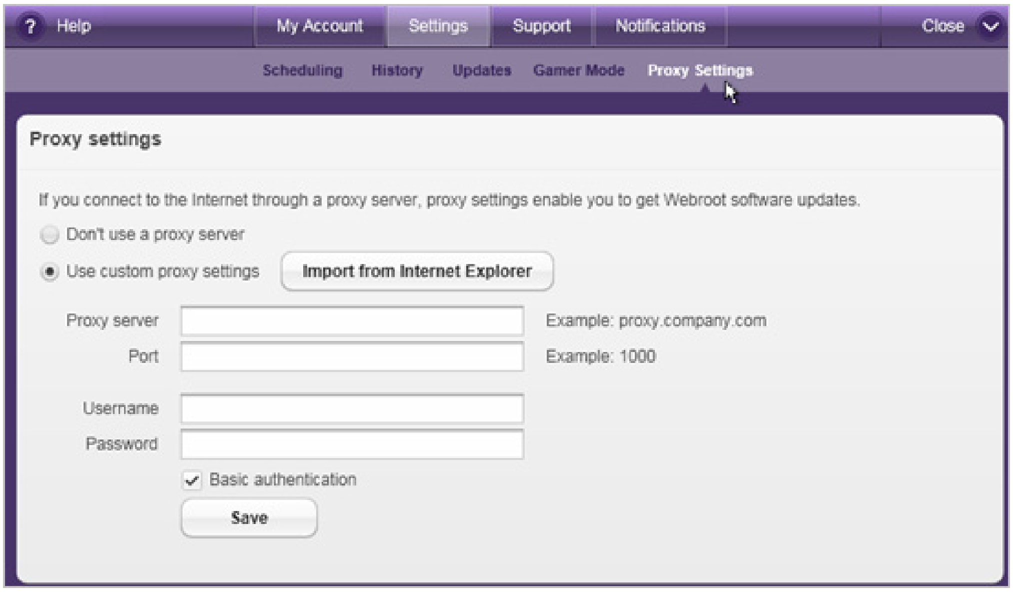
1. Open the Webroot main interface by double-clicking the Webroot icon in the system tray.
2. From the taskbar at the bottom of the Home panel, click **Settings**.



   The Settings panel opens.

3. Click **Proxy Settings**.

   The Proxy Settings panel opens.



Proxy settings

If you connect to the Internet through a proxy server, proxy settings enable you to get Webroot software updates.

○ Don't use a proxy server

● Use custom proxy settings

Proxy server Example: proxy.company.com

Port Example: 1000

Username

Password

☑ Basic authentication

4. Select the radio button next to **Use custom proxy settings**.

5. Define custom settings using one of the following methods.

Methods for defining proxy settings	
Use Internet Explorer settings	If you want to use values already defined in Internet Explorer, click the **Import from Internet Explorer** button.
Use your own settings	You can enter the proxy information, as follows: • **Proxy server**: Enter the fully qualified domain name of the server (for example, proxy.company.com). • **Port**: Enter the port number the server uses. • **Username and Password**: Enter the username and password for the server, if used. • **Basic authentication**: If the server uses another form of authentication besides basic Windows authentication, deselect the checkbox. **Note**: For further information about your proxy environment, contact your proxy server's administrator.

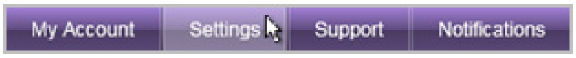
6. When you're done, click the **Save** button.

Changing the language setting

When you install the Webroot software, it automatically detects the language of your operating system and will use the same language for its own interface. If desired, you can change the language of the Webroot interface.

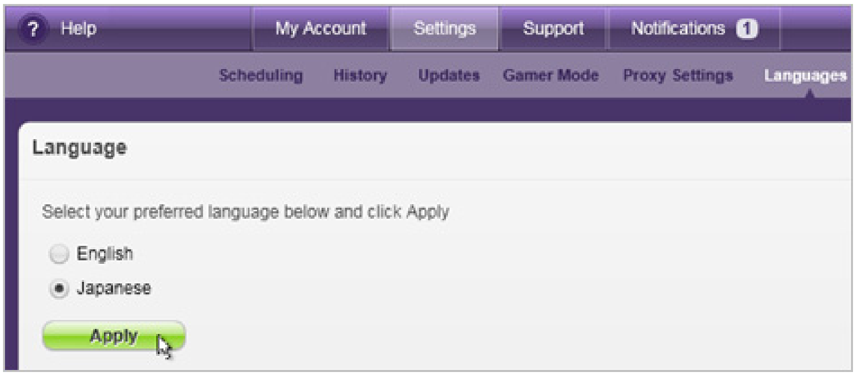
To change the language setting:

1. Open the Webroot main interface by double-clicking the Webroot icon in the system tray.
2. From the taskbar at the bottom of the Home panel, click **Settings**.



The Settings panel opens.

3. Click **Languages**.
4. Click the radio button for the desired language and click the **Apply** button.



Language

Select your preferred language below and click Apply

○ English
● Japanese

The program begins updating to the new language, a process that may take a few minutes.

A: Webroot Support

Webroot provides the following technical support services:

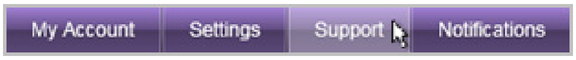
- **Web Site**. To submit a trouble ticket to our service representatives, access the Support Web site at support.webroot.com.

  We make every effort to respond to your request on the same day you send it in, but please allow up to 48 hours.

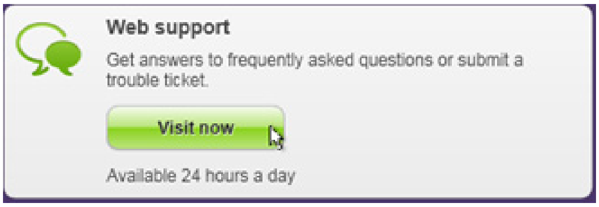
- **Phone**. For contact information, access the Support Web site at support.webroot.com.

To access technical support options:

1. Open the Webroot main interface by double-clicking the Webroot icon in the system tray.
2. From the taskbar in the bottom of the Home panel, click **Support**.



3. Click the **Visit now** button to open the Webroot Support site in your browser. (You must be connected to the Internet.) Or call the number listed to speak to a representative.



Web support

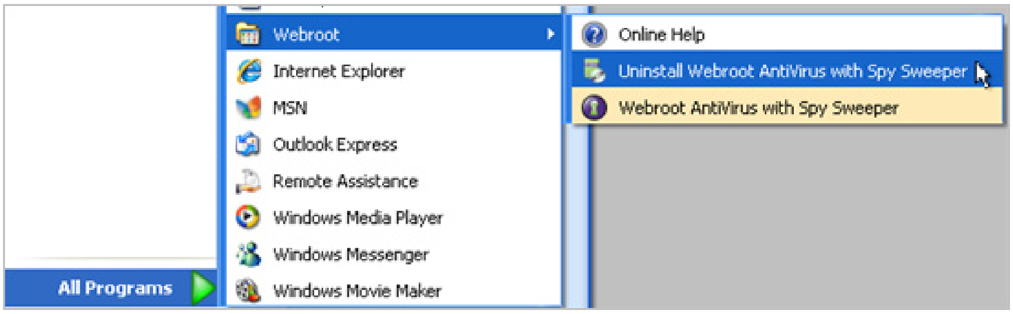
Get answers to frequently asked questions or submit a trouble ticket.

Available 24 hours a day

B: Uninstalling the program

To uninstall the Webroot software:

1. From the Start menu (click **Start** in the system tray), point to **All Programs**, then **Webroot**, then **Tools**, then **Uninstall Webroot AntiVirus with Spy Sweeper**.



   A Webroot dialog opens and begins removing the Webroot software files.

2. When the final dialog opens, click **Finish** to restart your computer.

C: Frequently Asked Questions

This appendix provides a list of frequently asked questions (FAQs), which are organized by the following topics:

- “Threat protection FAQs” on page 60
- “Scan and Quarantine FAQs” on page 61
- “Shield FAQs” on page 63
- “MyAccount FAQs” on page 64

Threat protection FAQs

What is malware and how does it get in my computer?

Malware is malicious software that is designed to harm your computer or compromise your privacy. If you do not have the Webroot software actively protecting your computer, malware can enter your computer through Internet connections, open computer ports, compromised disks, and email attachments. Internet connections are the primary source of entry. Whenever you connect to the Internet, you could provide the outside world with access to your computer and potentially allow in snoops, thieves, and virus outbreaks. Fortunately, Webroot blocks any threats before they can enter.

Note

The Webroot software acts like a personal security guard for your computer, blocking bad guys from entry and searching the premises for any others that may have slipped through the cracks. If it finds threats, it disables them and ejects them into Quarantine before they cause any harm.

The first time the System Scanner searches your computer, it may locate and quarantine many different types of threats that were previously running on your computer, probably without your knowledge. For detailed descriptions of the various types of malware, see the Glossary.

How do I know if my computer is infected?

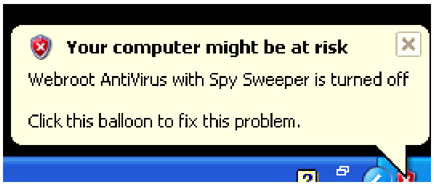
The Webroot software actively protects your computer from malware infections at all times. However, even with the best security protection, you can accidentally allow malware to gain access to your computer. This could happen if you clicked **Allow** in an alert screen for a program that you didn't realize was associated with malware.

If you notice any of the behaviors listed below, run a scan immediately (see "Scanning for threats" on page 14).

- If you see pornographic images or advertisements unexpectedly appear on your screen, you probably have a malware infection. Certain Web sites contain traps that take control of your browser and cause pornographic or advertising sites to open when you try to exit.
- Your computer is slow to boot, slow to process, crashes frequently, or behaves in erratic ways.
- You hear your hard disk actively working when you are not touching your computer.
- Numerous pop-up ads open even when you are not connected to the Internet.
- A different home page loads in your browser or strange entries appear in your Favorites and History.
- Strange results appear when you perform an Internet search.
- You can't access certain drives, programs, Web sites, or the printer.
- Strange messages or images open on your screen or music plays that you did not download.
- Strange icons appear on your desktop or strange programs appear in your start-up list.

Why does the Windows Security Center say that the Webroot software is turned off?

When you start your computer, you may see a pop-up alert from the Windows Security Center that says your computer is at risk and the Webroot software is turned off, similar to the example below.



Your computer might be at risk

Webroot AntiVirus with Spy Sweeper is turned off

Click this balloon to fix this problem.

Typically, this alert appears at Windows startup (and occasionally on shutdown) due to an overtaxed processor, low available system memory, or a high number of other startup items present on the system. Once the Webroot software has notified the Windows Security Center that it is up and running on your system, this alert should automatically close and you can ignore it. If the message persists longer than a few minutes, contact Webroot Support.

Scan and Quarantine FAQs

How do I know if the System Scanner found any threats?

In most cases, the Webroot software automatically manages threats for you by disabling them and moving them to Quarantine, where they can no longer harm your computer. You can view the Quarantine by opening the main interface, clicking **Edit settings** in the PC Security panel, and clicking the **Quarantine** tab.

If the software detects an item that it classifies as a potential threat or it does not recognize, it opens a pop-up alert and asks whether you want to accept the item or prevent it from installing on your computer.

You can also access a summary of Webroot software activity by clicking the arrow › next to **See how** on the Home panel.

How does Webroot know the difference between malware and legitimate programs?

When the System Scanner searches your computer, it checks installed programs and other items it finds against our database of security definitions. These definitions are a set of fingerprints that characterize viruses, spyware, adware, and other types of unwanted items. The Webroot Threat Research team constantly updates these definitions to protect your computer from ever-changing spyware and other potential threats. Webroot automatically downloads these definitions to your computer so you are always protected.

Can I work on my computer during a scan?

Yes, the System Scanner runs in the background without disrupting your work. If automated scanning is enabled, the System Scanner runs only when your computer is inactive. If you start working on your computer while a scan is in progress, it pauses and waits until the computer has been inactive again for 15 minutes, then resumes scanning where it left off.

Can I quickly scan a USB or CD?

Yes, even though the Webroot software is configured to automatically scan all areas of the computer, you can run a quick scan yourself for a selected area, such as a USB drive or CD. You can run a quick scan by doing either of the following:

- Targeting a specific file or folder in Windows Explorer. Right-click on the file or folder to open the pop-up menu, then select **Perform Secure Scan**. This is the quickest method.
- Customizing the scan options to search specific drives or file types. See "Customizing scan options" on page 19.

Are there times when I should run a scan myself?

In most cases, you should not need to launch a scan because the Webroot software is configured to run scans automatically and to actively block threats with shields. However, you may want to run a scan yourself in the following circumstances:

- Even if you don't surf high-risk sites, keep in mind that connecting to the Internet is like opening the front door to your computer. In most situations no one will walk through, but if you are not protected with the Webroot software, you are leaving your computer vulnerable to bad guys who might enter unannounced, snoop around your files, and wreck havoc on your applications.
- After you have surfed networking sites, adult-entertainment sites, free lyrics and music download sites, and other high-traffic sites. Malware writers are constantly re-engineering methods to infect computers. They commonly target popular Web sites by creating pop-up ads that can trick you into clicking on a link or by targeting you for a "drive-by download," where an infection will attempt to silently install on your computer as you view pages.
- If you accidentally clicked on a suspicious looking pop-up advertisement. Malware writers use all kinds of tricks to lure you into clicking a link and launching their spyware application.
- If you frequently download screen savers, music, games, movies, or pictures. Any time you download items on your computer, even legitimate ones, you could download malware along with it. Spyware commonly piggybacks on downloads and can install on your computer without your knowledge.

For scanning instructions, see "Scanning for threats" on page 14.

What should I do with items in Quarantine?

Once items are moved to Quarantine, your safest action is to simply keep them there. Items in Quarantine are disabled and cannot harm your computer. Keeping items in Quarantine also allows you to test your computer and determine if all your programs still work properly after the scan. If you discover that some legitimate programs cannot function after an item was moved to Quarantine, Webroot allows you to restore it.

What are cookies and why does it find so many?

Every time you access an Internet site, the server for that site may place small bits of text called cookies on your computer to store information about your interaction with it. If you have accessed many different sites, the System Scanner locates many different cookies. You should not be alarmed if the System Scanner finds a large number of cookies. Cookies do not pose a high risk for your computer's security, because they cannot harm your computer or steal information. However, while some cookies can be helpful to your Internet browsing experience, some third-party cookies can be a privacy concern because they are placed on your computer by a different Web site other than the one you accessed. Usually associated with on-line advertising, third-party cookies can be used to track your movements as you surf the Internet and to create a profile of your viewing habits.

Note

For Internet Explorer, cookies are stored as separate files. For Firefox, cookies are stored in one file.

Cookies are simple text files that store information about a Web site you visited. They do not create pop-up ads, nor can they launch viruses. In most cases, cookie files do not contain any private information such as credit card numbers.

The System Scanner mainly sweeps for third-party cookies associated with advertising, not the helpful first-party cookies that store your personal preferences for a particular Web site, such as login information and shopping cart items. If you want the System Scanner to ignore all cookies during scans, see “Customizing scan options” on page 19.

Shield FAQs

How do I know if I should block or allow a download?

If the Webroot Shields detect a potential threat, an alert opens and asks whether you want to allow the file to launch or block the file from launching. Information about the item is shown in the alert dialog. If you recognize the file name and you are purposely downloading it (for example, you were in the process of downloading a new toolbar for your browser), click **Allow** to continue. However, we recommend that you run an on-demand scan after downloading even legitimate items, since malware can piggy-back on any type of download. See “Scanning for threats” on page 14.

If you were *not* trying to download anything and were just viewing pages on the Internet, you should block the file. As you surf Internet sites, you could be targeted for a drive-by download, where an unwanted program launches and silently installs on your computer as you view pages.

A Windows dialog says it found spyware, but no Webroot alert appeared. What do I do?

Don’t click on it. Unfortunately, pop-up windows from an Internet site can be designed to look like legitimate messages from Windows with the sole purpose of trying to trick you. They display scary messages, such as “Warning! A Virus was Found on your Computer! Buy SomeSoftware now!” and have buttons and icons that look like actual Windows graphics.

Some of these fake messages are trying to lure you to another Web site where they will ask for your credit card number or other personal information. Others are advertisements designed to look like fake Windows dialogs (look for grayed-out text that says “advertisement” displayed in a bottom corner). The most evil aspect of these fake messages is that if you click anywhere in the dialog box, even on the **No** or **Close** button, you will execute its intended actions, such as launching malware or sending you to a rogue Internet site. The best way to remove a fake message from your screen is to press **Alt-F4** (hold down the **Alt** button while pressing the **F4** key).

But rest assured, even if you accidentally click on a fake dialog, the Webroot software blocks any malware, disables it, and sends it to Quarantine.

Do I need shields if a firewall is running?

Yes, you should keep both the firewall and the Webroot Shields enabled, since they are using different methods to locate different types of threats. The firewall looks for unrecognized communications over the computer ports, such as activity that may indicate hacking attempts. Shields look for specific programs and files that match Webroot's threat definitions, such as spyware and viruses, and stop them before they launch.

MyAccount FAQs

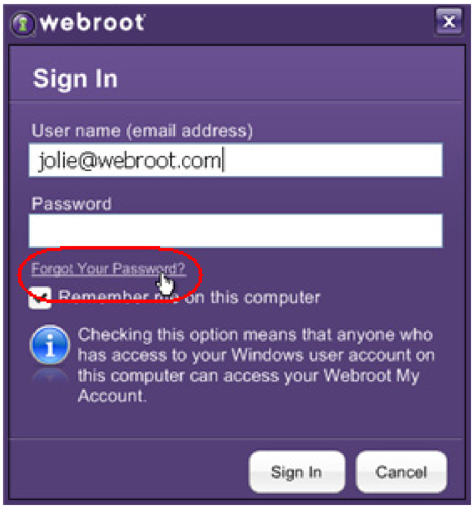
Can I install the Webroot software on another computer?

You can only install the Webroot software on another computer if you purchased a multi-user license. For more information, see "Managing licenses and additional products" on page 42.

Keep in mind that if you install the Webroot software on additional computers, these installations will all share a single Webroot account in *My Webroot*. This means that anyone using the other computers can sign in to your online account at **http://www.webroot.com/mywebroot**. If you have personal information that you do not want to share in your online account, do not provide others with your user name and master password.

What should I do if I forget my account password?

If you forget your original password, you can create a new one. To reset your password, right-click the Webroot icon in the system tray and click **Sign In** from the pop-up menu. Click the link for **Forgot Your Password?**. (You must be connected to the Internet.)



User name (email address): jolie@webroot.com

Password:

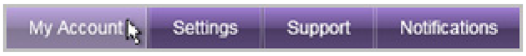
☑ Remember me on this computer

Checking this option means that anyone who has access to your Windows user account on this computer can access your Webroot My Account.

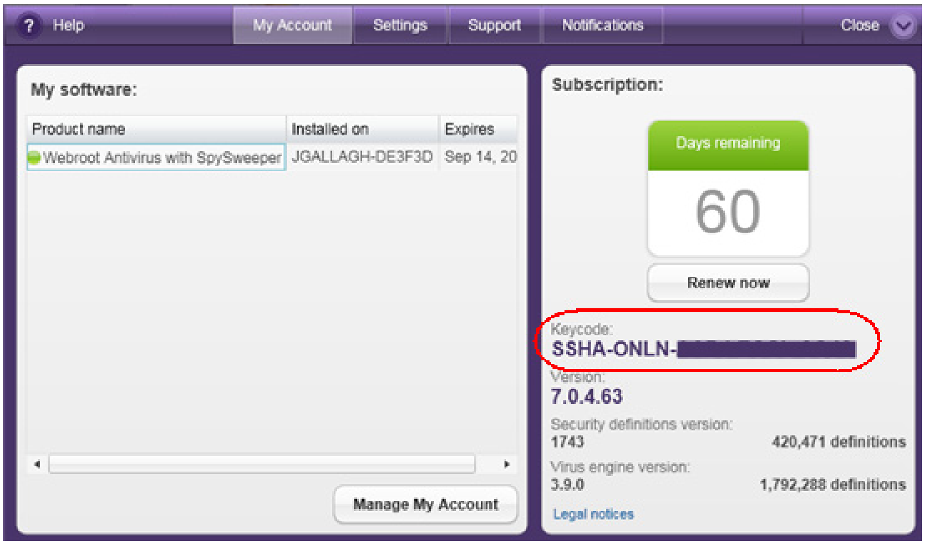
When the Reset Password page appears, enter your email address and click **Send Email**. Webroot sends you an email with instructions for resetting your password.

How do I find my keycode?

To view the keycode for your software license, open the Webroot main interface by double-clicking the Webroot icon in the system tray. From the taskbar at bottom of the Home panel, click **My Account**.



The My Account panel opens and shows your keycode to the right.



My software:

Product name	Installed on	Expires
Webroot Antivirus with SpySweeper	JGALLAGH-DE3F3D	Sep 14, 20

Subscription:

60

Keycode:
SSHA-ONLN-[redacted]

Version:
7.0.4.63

Security definitions version:
1743 420,471 definitions

Virus engine version:
3.9.0 1,792,288 definitions

Can other users access my online account?

No one can access your account unless they know your Webroot master password. However, if you installed the Webroot software on additional computers, these installations will all share a single Webroot account. This means that anyone using these other computers can sign in to your online account if they know your user name and password. If you have personal information in your account that you do not want to share, do not provide other members in your household with your user name and master password.

Can multiple users access the Webroot software from one computer?

Yes, if your computer is configured for multiple Windows user accounts (each person logs in with a unique name and password), the Webroot software is available to all those users. Each user with administrative privileges has full access to all areas of the Webroot software, while other users have limited access. The Webroot software continues its threat protection activities, no matter which user is logged into the computer.

Glossary

ActiveX

ActiveX technology was developed by Microsoft to allow Web browsers to download and execute programs on your computer. ActiveX controls have many legitimate uses, such as running animations, triggering sounds, or downloading Microsoft updates. However, many spyware programs also use ActiveX to install themselves on your computer. If you see an ActiveX alert, you should block it from running, unless you trust the source of the ActiveX technology.

adware

Adware is a type of software that may display advertisements on your system. Some adware may also hijack Web searches, meaning it may reroute your Web searches through its own Web page. It may change your default home page to a specific Web site. Adware generally propagates itself using dialog boxes, various social engineering methods, or through scripting errors.

Alternate Data Stream (ADS)

An Alternate Data Stream is a highly technical way to hide images, data, or code in a file and can be used to hide malicious code. The hidden content is impossible to detect using regularly available tools, such as Windows Explorer.**Browser Helper Objects (BHOs)**

Browser Helper Objects are add-on programs that work with Internet Explorer. BHOs have many legitimate uses, such as allowing you to display a PDF file within your browser or to install a search box for your toolbar. However, many spyware programs also use BHOs to display ads, track your Internet activity, or hijack your home page. If a BHO alert opens while you are intentionally downloading a new toolbar or other plug-in, you can allow the installation. Otherwise, block it.

cookies

Cookies are small text files generated by a Web server and then stored on your computer for future use. (For Internet Explorer, cookies are stored as separate files. For Firefox, cookies are stored in one file.) Cookies can contain everything from tracking information about sites you visited to your personal preferences. Cookies cannot steal information off your machine, but some do store personal information that you may not want outside parties to gather. The System Scanner only searches for third-party cookies associated with advertising sites that may be gathering information about your surfing habits.

definitions

A security definition is a set of fingerprints that characterize viruses, spyware, adware, or other types of unwanted items. Webroot regularly updates these definitions to provide better protection against the latest versions of these security threats.

dialer

Dialers are software packages that connect your computer to the Internet via a modem hooked to a phone jack. Malicious dialers may disconnect your computer from your Internet Service

Provider (ISP) and reconnect you to the Internet using an expensive toll or international phone number. They can accrue significant phone charges and can run in the background, hiding their presence. They generally propagate themselves using dialog boxes, various social engineering methods, through scripting errors, or may be delivered with a Trojan horse.

firewall

A firewall monitors data traffic traveling in and out of your computer's ports. It can eliminate unauthorized access to your computer at home, at the office, or on the road. Using a multi-layered approach to defense, Webroot's firewall can block malware, hacking attempts, and other online threats before they can enter and cause damage to your system.

host name

A host name identifies a device connected in the Internet. Computers on the Internet are often named WWW. Computers on a network are usually single names that describe the computer, such as "accounting1." Host names can be part of a fully qualified domain name (FQDN). For example, in "www.webroot.com," the "www" is the host name and "webroot.com" is the domain name.

hosts file

The Hosts file is a Windows file that helps direct your computer to a Web site using Internet Protocol (IP) addresses. Your Web browser uses the IP address to actually connect to a site. When you enter a Web address in a browser, your computer first looks in the Hosts file to see if it already knows where to go. If the domain is listed (for example, webroot.com), your computer goes directly to the IP address. If the domain is not listed, your computer looks up the information from the Internet (a slightly slower process).

HTML

Hyper**T**ext **M**arkup **L**anguage is a method used to display content in Web pages.

HTTP

Hyper **T**ext **T**ransfer **P**rotocol is a set of rules for transferring files (text, graphics, sound, etc.) on the World Wide Web. As soon as you open a Web browser, you are indirectly using HTTP.

IP address

An **I**nternet **P**rotocol address identifies a machine (computer or server) on the Internet. The address is a series of four numbers separated by periods (for example, 64.78.182.210). Your own computer's IP address may be the same address during every Internet connection (called a *static IP*, used in most T1/DSL connections) or it may change for each Internet connection (called a *dynamic IP,* used in most cable/dial-up connections).

keylogger

A keylogger is a type of system monitor that has the ability to record all keystrokes on your computer. It may monitor keystrokes, emails, chat room dialogue, instant message dialogue, Web sites visited, usernames, passwords, programs run, and any other typed material. They have the ability to run in the background, hiding their presence. Keyloggers and system monitors may be used for legitimate purposes, but can also be installed by a user to record sensitive information for malicious purposes.

malware

Malware is short for **"mal**icious soft**ware**," which is designed to destroy or harm your computer system, such as a virus.

POP3

Post **O**ffice **P**rotocol 3 is a standard protocol that allows you to receive email and store it in an Internet server. Most email applications use POP3.

ports

Ports are numbers that identify the entry and exit points of your computer. Computers divide one physical port connection into thousands of virtual port connections, most of which are never used. All communications protocols have designated entrance ports to your computer. For example, traffic sent using HTTP for Web pages generally travels through port 80. Your computer's ports are either open or closed. An open port allows any information to flow through it and can make your computer vulnerable to hackers. A closed port blocks incoming traffic.

proxy server

A proxy server is a computer system or router that acts as a relay between a client and server. Proxy servers are used to help prevent an attacker from invading the private network and are often used in building a firewall.

Quarantine

Quarantine is a holding area for spyware, viruses, and other potentially unwanted applications during a sweep. The quarantine process does not delete items from your computer. Rather, it renders them inoperable and stores them in a safe place where they cannot cause any harm to your computer. Items in quarantine can be deleted or restored to their original locations.

random access memory (RAM)

RAM is the main memory that acts as the computer's workspace for running programs. Spyware and other unwanted programs can steal the computer's memory resources, which can lead to system crashes, slower performance, or instability.

registry

A registry is a database of hardware and software settings about your computer's configuration, such as the types of programs that are installed. Spyware can create entries in the Windows registry, which can ultimately slow down your computer and cause problems in your system.

rootkit

A rootkit is a collection of tools that enable administrator-level access to a computer or network. By using file-obfuscation techniques, rootkits can hide logins, processes, files and logs, and may include software to capture information from desktops or a network. Spyware developers often use rootkits to avoid detection and removal.

scan

A scan is the process of searching for potential threats on your computer, such as spyware and viruses, then moving those items to Quarantine.

shields

Webroot shields continuously monitor activity related to your Web browser settings, network communications between your computer and Web sites, Windows system settings, Windows Startup programs, and email attachments. If the shields detect spyware or any other potential threats attempting to download, they will either move the item to quarantine or open an alert message that asks you to take action.

SMTP

Simple **M**ail **T**ransport **P**rotocol is a method used for sending text-based information (email). Because SMTP is limited in its receiving functions, it is often used with two other protocols, POP3 or IMAP. These protocols let you save messages in a server mailbox and download them periodically from the server.

spam

Spam is unsolicited junk mail sent to your email address. Its sole purpose is to lure you into buying their product or service. The term “spam” originated with a Monty Python sketch and song, the lyrics of which kept repeating the words, “SPAM, SPAM, SPAM...”, much like endless, unwanted email.

spy cookie

A spy cookie is a Webroot term for a third-party cookie associated with advertising sites that may be gathering information about your surfing habits.

spyware

Spyware is a program that may either monitor your online activities or possibly install programs without your consent. Information about online activities may be subsequently sent to a third party for malicious purposes without your knowledge. Spyware may arrive bundled with freeware or shareware, through email or instant messenger, may propagate itself using dialog boxes, various social engineering methods, scripting errors, or by someone with access to your computer.

system monitors

System monitors, typically non-commercial, may monitor and capture your computer activity, including recording all keystrokes, emails, chat room dialogue, instant message dialogue, Web sites visited, usernames, passwords, and programs run. These programs are capable of taking screen shots of your desktop at scheduled intervals and storing the information on your computer in an encrypted log file for later retrieval. A system monitor can run in the background, hiding its presence. These programs typically install via other threats, such as music downloads and Trojan downloaders.

traces

Traces are individual elements that make up the security definition database. The more traces found and put into the definitions, the more complete the removal of the potential threats.

Trojan horses

A Trojan horse may take control of your computer files by using a program manager that allows a hacker to install, execute, open, or close programs. It can run in the background, hiding its presence. A Trojan is usually disguised as a harmless software program and may also be distributed as an email attachment. Opening the program or attachment may cause an auto-installation process that loads the downloader onto your computer and download third-party programs on your computer, resulting in the installation of unwanted programs without your knowledge or consent. Trojans can also open a port on your computer that enable a hacker to gain remote control of your computer.

URL

Uniform **R**esource **L**ocator (URL) is the unique address for a file that is accessible on the Internet. To access the home page of a Web site, you can enter the URL of the home page (for example: http://www.webroot.com) in the browser’s address line. You can also access specific files using URLs (for example: ftp://www.webroot.com/sample.txt). The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies a specific computer on the Internet, and a pathname for a specific file.

virus

A virus is a self-replicating program that can infest computer code, documents, or applications. While some viruses are purposefully malignant, others are more of a nuisance, replicating uncontrollably and inhibiting system performance.

virus cleaning

Virus cleaning is a Webroot procedure that removes infected portions of a file, when a virus is detected during a sweep. If the Webroot software can remove the virus successfully, it restores the cleaned file to your computer in its original location and places a copy of the corrupted file in Quarantine. The cleaned file is safe to use; the file in Quarantine is not safe to use.

Index